# Table of Contents

1. **Introduction** .................................................................................................................. 7  
   1.1. Purpose ........................................................................................................................ 7  
   1.2. Scope ........................................................................................................................... 7  
   1.3. Owner ........................................................................................................................... 7  
   1.4. Document Structure ..................................................................................................... 7  

2. **Security Policy** ............................................................................................................... 8  
   2.1. Information Security policy document ............................................................................ 8  
   2.2. Review of Information security policy .............................................................................. 9  
   2.3. Information Security Policy of Oil India ........................................................................... 9  

3. **Organisational Security** .................................................................................................. 10  
   3.1. Internal Organization ..................................................................................................... 10  
      3.1.1. Management commitment to information security .................................................... 11  
      3.1.2. Information security co-ordination ......................................................................... 12  
      3.1.3. Allocation of information security responsibilities .................................................. 12  
      3.1.4. Authorization process for information processing facilities .................................. 13  
      3.1.5. Confidentiality agreements ..................................................................................... 13  
      3.1.6. Contact with authorities ........................................................................................ 13  
      3.1.7. Contact with special interest groups ....................................................................... 14  
      3.1.8. Independent review of information security ............................................................. 14  
   3.2. External parties ............................................................................................................... 14  
      3.2.1. Identification of risks related to external parties ......................................................... 14  
      3.2.2. Addressing security when dealing with customers .................................................... 14  
      3.2.3. Addressing security in third party agreements ........................................................ 15  

4. **Asset management** ........................................................................................................ 15  
   4.1. Responsibility for assets ............................................................................................... 15  
      4.1.1. Inventory of assets .................................................................................................... 15  
      4.1.2. Information Owners ................................................................................................. 16  
      4.1.3. Information Custodian ............................................................................................. 17  
      4.1.4. Acceptable use of assets .......................................................................................... 17  
   4.2. Information classification ............................................................................................... 18  
      4.2.1. Classification guidelines .......................................................................................... 18  
      4.2.2. Information labelling and handling ........................................................................ 19  

5. **Human Resources Security** ............................................................................................ 19  
   5.1. Prior to employment ...................................................................................................... 19  
      5.1.1. Roles and responsibilities ......................................................................................... 19  
      5.1.2. Screening ................................................................................................................ 20  
      5.1.3. Terms and conditions of employment .................................................................... 20  
   5.2. During employment ...................................................................................................... 20
# OIL-IS-POL-IS-1.0 (Information Security Policy)

5.2.1. Management responsibilities ................................................................. 20
5.2.2. Information security awareness, education, and training ....................... 21
5.2.3. Disciplinary process .............................................................................. 21
5.3. Termination or change of employment ....................................................... 21
  5.3.1. Termination responsibilities ................................................................ 21
  5.3.3. Removal of access rights .................................................................... 22
6.1. Secure areas .............................................................................................. 22
  6.1.6. On-site and off-site backups ................................................................. 24
  6.1.5. Information backup testing .................................................................. 24
  6.1.4. Information back-up ........................................................................... 24
  6.1.3. Controls against mobile code ............................................................... 25
  6.1.2. Controls against malicious code .......................................................... 25
  6.1.1. System acceptance ............................................................................ 26
6.2. Equipment security .................................................................................... 24
  6.2.7. Equipment sitting and protection ......................................................... 24
  6.2.6. Supporting utilities .............................................................................. 24
  6.2.5. Cabling security .................................................................................. 25
  6.2.4. Equipment maintenance ................................................................. 25
  6.2.3. Security of equipment off-premises ...................................................... 25
  6.2.2. Secure disposal or re-use of equipment .............................................. 26
  6.2.1. Removal of property .......................................................................... 26
7. Communications and Operations Management .............................................. 26
  7.1. Operational procedures and responsibilities ............................................ 26
    7.1.1. Documented operating procedures .................................................. 26
    7.1.2. Change management ....................................................................... 27
    7.1.3. Segregation of duties ...................................................................... 28
    7.1.4. Separation of development, test, and operational facilities ............ 28
  7.2. Third party service delivery management ................................................. 29
    7.2.1. Service delivery .............................................................................. 29
    7.2.2. Monitoring and review of third party services .................................. 29
    7.2.3. Managing changes to third party services ....................................... 29
  7.3. System planning and acceptance ............................................................... 30
    7.3.1. Capacity management .................................................................... 30
    7.3.2. System acceptance ........................................................................... 30
  7.4. Protection against malicious and mobile code .......................................... 31
    7.4.1. Controls against malicious code ...................................................... 31
    7.4.2. Controls against mobile code ............................................................ 32
  7.5. Back-up .................................................................................................. 32
    7.5.1. Information back-up ....................................................................... 32
    7.5.2. Information backup testing .............................................................. 32
    7.5.3. On-site and off-site backups ............................................................. 32
OIL-IS-POL-IS-1.0 (Information Security Policy)

7.5.4. Security requirement for backup tapes in transit .................................................. 33
7.5.5. Labelling of backup tapes ..................................................................................... 33
7.5.6. Information Restore .............................................................................................. 33
7.6. Network security management .................................................................................. 33
7.6.1. Network controls .................................................................................................. 33
7.6.2. Security of network services ................................................................................ 35
7.7. Media handling .......................................................................................................... 35
7.7.1. Management of removable media ....................................................................... 35
7.7.2. Disposal of media ................................................................................................. 35
7.7.3. Information handling procedures ........................................................................ 36
7.7.4. Security of system documentation ...................................................................... 36
7.8. Exchange of information .......................................................................................... 36
7.8.1. Information exchange policies and procedures .................................................. 36
7.8.2. Exchange agreements ........................................................................................... 37
7.8.3. Physical media in transit ...................................................................................... 37
7.8.4. Electronic messaging ............................................................................................ 38
7.8.5. Internet Usage Policy ........................................................................................... 39
7.8.6. Business information systems ............................................................................ 40
7.9. Electronic commerce services .................................................................................. 41
7.9.1. Publicly available information ............................................................................. 41
7.10. Monitoring ................................................................................................................ 41
7.10.1. Audit logging ...................................................................................................... 41
7.10.2. Monitoring system use ....................................................................................... 41
7.10.3. Protection of log information ............................................................................ 42
7.10.4. Administrator and operator logs ........................................................................ 42
7.10.5. Fault logging ....................................................................................................... 42
7.10.6. Clock synchronization ......................................................................................... 43
8. Access Control .............................................................................................................. 43
8.1. Business requirement for access control .................................................................. 43
8.1.1. Access control policy ........................................................................................... 43
User access management ................................................................................................. 44
8.1.2. User registration ................................................................................................... 44
8.1.3. Privilege Management of employees ................................................................ 44
8.1.4. Privilege Management of non-employees .......................................................... 45
8.1.5. User password management ................................................................................ 45
8.1.6. Review of user access rights ............................................................................... 46
8.2. User responsibilities ................................................................................................ 46
8.2.1. Password use ....................................................................................................... 46
8.2.2. Unattended user equipment ................................................................................. 46
8.2.3. Clear desk and clear screen policy ...................................................................... 47
8.3. Network access control ............................................................................................ 47
9. **Information Systems Acquisition, Development and Maintenance**

9.1. **Security requirements of information systems**

9.1.1. **Security requirements analysis and specification**

9.2. **Correct processing in applications**

9.2.1. **Input data validation**

9.2.2. **Control of internal processing**

9.2.3. **Message integrity**

9.2.4. **Output data validation**

9.3. **Cryptographic controls**

9.3.1. **Policy on the use of cryptographic controls**

9.3.2. **Key management**

9.4. **Security of system files**

9.4.1. **Control of operational software**

9.4.2. **Protection of system test data**

9.4.3. **Access control to program source code**

9.5. **Security in development and support processes**

9.5.1. **Change control procedures**

9.5.2. **Technical review of applications after operating system changes**

9.5.3. **Restrictions on changes to software packages**

9.5.4. **Information leakage**

9.5.5. **Outsourced software development**

9.6. **Technical vulnerability management**

9.6.1. **Control of technical vulnerabilities**
10. Information Security Incident Management

10.1. Reporting information security events and weaknesses

10.1.1. Reporting information security events

10.1.2. Reporting security weaknesses

10.2. Management of information security incidents and improvements

10.2.1. Responsibilities and procedures

10.2.2. Learning from information security incidents

10.2.3. Collection of evidence


11.1. Information security aspects of business continuity management

11.1.1. Including information security in the business continuity management process

11.1.2. Business continuity and risk assessment

11.1.3. Developing and implementing continuity plans including information security

11.1.4. Business continuity planning framework

11.1.5. Testing, maintaining and re-assessing business continuity plans

12. Compliance

12.1. Compliance with legal requirements

12.1.1. Identification of applicable legislation

12.1.2. Intellectual property rights (IPR)

12.1.3. Protection of organizational records

12.1.4. Data protection and privacy of personal information

12.1.5. Prevention of misuse of information processing facilities

12.2. Compliance with security policies and standards, and technical compliance

12.2.1. Compliance with security policies and standards

12.2.2. Technical compliance checking

12.3. Information systems audit considerations

12.3.1. Information systems audit controls

12.3.2. Protection of information systems audit tools

13. Non Compliance
1. Introduction

1.1. Purpose

This document defines the Company’s position on information security. The policy is applicable across the Company and is also subject to amendment at any time depending upon the changes in business requirements or environment with requisite approvals.

This objective of this policy is to describe the security requirements for information assets belonging to Oil India, used across the Company. These assets can be in written, spoken or computer-based form and the protection and security of these assets from unauthorized disclosure, misrepresentation, loss or wrongful use is of vital importance. Management and staff must ensure the Confidentiality, Integrity and Availability of all information assets, as required.

The information security policy as stated in this document supports the following three objectives -

- Provide management direction and support for information security;
- Support the security requirements of the business; and
- Build business partnership/relations confidence.

1.2. Scope

This policy supports the organization’s Information Security Policy Statement as stated in OIL-IS-ISMS ISM-1.0 (ISMS Manual). The scope of the Information Security Policy is as specified in the Scope Document (OIL-IS-ISMS-SD-1.0 (Oil India Scope Document)).

1.3. Owner

The Chief Information Security Officer (CISO) is the owner of this policy and will be responsible for reviewing and updating the policy as and when required based on the change in the business requirements or environment. The CISO will also ensure that the updated policy is implemented across the organization.

1.4. Document Structure

For easy reference, this document is structured following the 11 security categories of ISO 27001 standard:

- Security Policy;
OIL-IS-POL-IS-1.0 (Information Security Policy)

- Organisation of Information Security;
- Asset Management;
- Human Resources Security;
- Physical and Environmental Security;
- Communications and Operations Management;
- Access Control;
- Information Systems Acquisition, Development and Maintenance;
- Information Security Incident Management;
- Business Continuity Management; and
- Compliance.

2. Security Policy

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

2.1. Information Security policy document

- The information security policy will provide management direction and support to information security.
- The information security policy will be communicated throughout the organization to users in a form that is relevant, accessible and understandable to the intended audience.
- The policy will explain the policies, principles and compliance requirements for particular importance to the organization, including:
  - Legislative, regulatory, and contractual compliance;
  - Security education, training, and awareness requirements;
2.2. Review of Information security policy

- Major changes in the IS Policy will need approval from the ISC. ISC will decide whether further approval from the Company’s Board of Directors is required and will put up the proposal to the Board accordingly.

- Minor changes in day-to-day activities/ functions/ procedures will be approved by the ISWG and published company-wide, with information to ISC. These changes may be related to the aspects mentioned below.

- Initial review will be carried out by the ISWG and, if necessary, put up to the ISC for approval.

- The review will include, but not limited to:
  - Feedback from business users;
  - Change in the business;
  - Change in the IT environment;
  - Trends related to threat and vulnerabilities; and
  - Reported security incidents.

- Records for the management review and approval will be maintained.

2.3. Information Security Policy of Oil India

Oil India’s Information Security Policy commits the Company to protect the security of its Information. It provides the same commitment to information entrusted to Oil Indiaby its customers and business partners. We will deliver the above components in an integrated...
manner thorough an Information Security Management System that protects the *Confidentiality, Integrity and Availability* of Oil India’s information.

To meet this commitment we will:

- Maintain an effective Information Security Management System;
- Deploy most appropriate technology and infrastructure;
- Create and maintain a security conscious culture within Information Services; and
- Continually monitor and improve the effectiveness of the Information Security Management System.

Responsibility for compliance with Oil India’s Security Policy and standards lies with HEAD-IT or CISO and their staff.

### 3. Organisational Security

**Objective:** To manage information security within the organisation.

**3.1. Internal Organization**

The organization of ISMS will be enforced by:

- Establishing a management framework to initiate and control the implementation of information security within the organization.
- Ensuring that a governance framework is developed to maintain information security within the organization; and
- Assigning the security roles and co-ordinating the implementation of security across the organization.

Management will approve the information security policy, assign security roles and co-ordinate and review the implementation of security across the organization.
3.1.1. Management commitment to information security

- The Information Security Council (ISC) will be formed comprising of senior management representation from all the major departments as IT, Operations, Finance, Legal and Human Resource, Facility, corporate etc. The roles and responsibilities of ISC will include:
  
  o periodic review of information security at Oil India;
  o review of security incident monitoring processes within the Company;
  o approval and review of information security projects;
  o approval of new or modified information security policies;
  o performing other necessary high-level information security management activities;
  o ensuring that there is clear direction and visible management support for security initiatives in place; and
  o Promoting security through appropriate commitment and adequate resourcing.

- The Information Security Working Group (ISWG) will be formed comprising of individuals responsible for implementing and maintaining the information security policies and procedures across the organization. The roles and responsibilities of ISWG will include:
  
  o reviewing effectiveness of the implementation of the information security policy;
  o approving assignment of specific roles and responsibilities for information security across the organization;
  o initiating plans and programs to maintain information security awareness; and
  o ensuring that the implementation of information security controls is co-ordinated across the organization.
The organizational structure of ISC and ISWG has been detailed in the Information Security Organization. The Information Security Council will meet at least once a year to assess the security requirements of Oil India or as required by any significant change in the business operating environment. Members of ISC may depute their representative for mandatory review meetings.

3.1.2. Information security co-ordination

- Company management will ensure an effective coordination of information security activities across the organization between various department including Human Resources, Information Technology, Legal, Finance and Business Operations. The activities ensure that:
  
  o information security policy is complied to;
  
  o all non-compliances to information security policy are addressed;
  
  o significant changes in threats and exposure to information and information processing facilities are identified; and
  
  o Information security incidents are identified and addressed appropriately.

3.1.3. Allocation of information security responsibilities

- Information security roles and responsibilities for the members of ISC and ISWG will be clearly defined and documented.

- Information asset owners will be responsible for the security of the information asset and for identifying and implementing the controls that are necessary to protect the asset.

- The Chief Information Security Officer will perform the quarterly compliance checks, or get it carried out by trusted third parties, to ensure that all information security policies and processes are complied by across the organization.
3.1.4. Authorization process for information processing facilities

- A formal risk assessment will be performed by ISWG and approved by the ISC for new technologies to be used in the Company production information system.

- Critical components of the Company’s information security infrastructure will not be disabled, bypassed, turned off, or disconnected without prior approval from ISWG.

3.1.5. Confidentiality agreements

- Users will sign agreement highlighting confidentiality requirements as part of their initial terms and conditions of employment.

- Without specific written exceptions, all programs and documentation generated by, or provided by any employee for the benefit of the Company are the property of the Company and all employees providing such programs or documentation will sign a statement to this effect prior to the provision of these materials.

- Whenever communications with third parties necessitate the release of the Company’s sensitive information, a standard Non-Disclosure Agreement (NDA) or confidentiality clause, authorised by the Company’s Legal department, will be signed by the third party.

3.1.6. Contact with authorities

- Appropriate procedures will be defined to specify when and which authorities (law enforcement, fire department, supervisory authorities) will be contacted whenever required.

- An updated list of authorities with appropriate contact details will be maintained and available to required personnel at all times.

- Every decision involving law enforcement regarding information security incidents or problems must be made by the ISC.

- Unless compelled by law to disclose attacks against its computer systems or networks, the Company will not report these incidents to the public or any government agency.
3.1.7. Contact with special interest groups

– Appropriate contacts with special interest groups or other security forums and professional associations will be formed to maintain and improve the knowledge of good practices and receive early warning of alerts, advisories and patches in order to reduce vulnerabilities.

3.1.8. Independent review of information security

– An independent review of information security policy and associated controls will be performed:
  o internally every six months

3.2. External parties

3.2.1. Identification of risks related to external parties

– The risks associated with access to the Company’s internal systems by third parties will be assessed and appropriate security controls implemented.

– When using an external contractor to manage information processing facilities, risks will be identified in advance, mitigating controls will be identified and established, and contractor expectations will be incorporated into the contract for these services.

3.2.2. Addressing security when dealing with customers

All customers shall be provided with information on security best practices followed to enhance security while using information resources. The following requirements shall be addressed prior to granting access to the customers:

  o The level of access required for the customers and the list of users requiring access;

  o Justification, requirements and benefits for customer access;

  o Protection of IPR and joint IPR held with the customer;
The contractual right to monitor, revoke any activity related to company’s assets;

- Respective Liabilities of the organization and the customer; and

- The above-mentioned requirements shall be documented and signed by the customer and company. These requirements shall be incorporated in the contractual agreement with the client.

The Company will not publicly disclose any information related to a business deal or transaction that could reasonably be expected to be materially damaging to a customer or another third party.

3.2.3. **Addressing security in third party agreements**

- The security requirements of outsourcing the management and control of all or some of the Company’s information systems, networks and/or desktop environments will be addressed in a contract agreed between the parties.

4. **Asset management**

**Objective:** To achieve and maintain appropriate protection of organizational assets.

4.1. **Responsibility for assets**

4.1.1. **Inventory of assets**

- Information assets at the Company will be classified based on the impact on the organization, due to loss of their confidentiality, availability and integrity.

- An inventory of all critical information assets will be drawn up and maintained to ensure appropriate protection of Company’s information assets. The asset inventory will include all information necessary in order to recover from a disaster, including type of asset, backup information, license information, security classification and business value.
4.1.2. **Information Owners**

- An owner will be identified for each of the information assets at the Company. The owner will be responsible for:
  
  o ensuring that information and assets associated with information processing facilities are appropriately classified; and
  
  o defining and periodically reviewing access restrictions and classifications, taking into account applicable access control policies.

- Information Asset owners or their delegates will be responsible for the following activities:
  
  o approve information-oriented access control privileges for specific job profiles;
  
  o approve information-oriented access control requests that do not fall within the scope of existing job profiles;
  
  o select special controls needed to protect information, such as additional input validation checks or more frequent backup procedures;
  
  o define acceptable limits on the quality of their information, such as accuracy, timeliness, and time from capture to usage;
  
  o approve all new and different uses of their information;
  
  o approve all new or substantially-enhanced application systems that use their information before these systems are moved into production operational status;
  
  o review reports about system intrusions and other events that are relevant to their information;
  
  o select a sensitivity classification category relevant to their information, and review this classification every year for possible downgrading or upgrading; and
  
  o select a criticality category relevant to their information so that appropriate contingency planning can be performed.
Information Owners will designate a back-up person to act if they are absent or unavailable. Owners will not delegate ownership responsibilities to third-party organizations such as outsourcing organizations, or to any individual who is not a full-time employee of the Company.

### 4.1.3. Information Custodian

- The information asset owner will identify a custodian for the information asset.
- The Custodian is in physical or logical possession of information and information systems and will perform the following activities:
  - follow the instructions of Owners, operate systems on behalf of Owners to serve users authorized by Owners;
  - define the technical options, such as information criticality categories, and permit Owners to select the appropriate option for their information;
  - define information systems architectures and provide technical consulting assistance to Owners so that information systems can be built and run to optimal meet business objectives;
  - if requested, provide reports to Owners about information system operations and information security issues; and
  - safeguard the information in their possession, including implementing access control systems to prevent inappropriate disclosure, and developing, documenting, and testing information systems contingency plans.

### 4.1.4. Acceptable use of assets

- All employees will have a personal responsibility for safeguarding all proprietary information, which includes but is not restricted to Sensitive documents and information, from disclosure to unauthorized parties.
4.2. Information classification

4.2.1. Classification guidelines

– Information assets of the organization will be classified based on their relative business value, legal requirements and impact due to loss of confidentiality, availability and integrity of the information asset.

– The level of security will be identified based on the information classification performed.

– Assets shall be grouped under the following asset types:
  
  - Physical assets
  - Software assets
  - Information assets
  - Services assets
  - People assets

– The information assets will be classified in the following four categories:
  
  - **Restricted**: Information that is highly sensitive and is available only to specific, named individuals (or specific positions).

  - **Confidential**: Information that is sensitive within the Company/Business and available only to a specific function, group or role.

  - **Internal**: Information that is sensitive outside the Company/Business and needs to be protected. Authorized Access to employees, contractors, sub-contractors and agents on a "Need to Know Basis" for Business related Purposes.

  - **Public**: Public Information (including information deemed public by legislation or through a policy of routine disclosure), available to the Public, all employees, contractors, sub-contractors and agents.
– If information is not marked with one of these categories, it will default into the “Internal” category.

4.2.2. Information labelling and handling

– The owner or creator of information will assign an appropriate label to the information, and the user or recipient of this information will consistently maintain an assigned label.

– Labels for sensitive information will appear on the outside of floppy disks, magnetic tape reels, CD-ROMs, audiocassettes, and other storage media. If a storage volume such as a floppy disk contains information with multiple classifications, the most sensitive category will appear on the outside label.

– Making additional photocopies or printing extra copies of information classified as ‘Sensitive’ information will not take place without the prior permission/approval of the Information Owner.

– Sensitive information on paper such as print outs, writing, fax etc. will be personally delivered to the designated recipients. Such output will not be delivered to an unattended desk or left out in open in an unoccupied office.

5. Human Resources Security

Objective: To ensure that users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.

5.1. Prior to employment

5.1.1. Roles and responsibilities

– Users will fulfil all security roles and responsibilities as laid down in this Information Security Policy.
5.1.2. Screening

– Background screening, as required for the role, on permanent staff will be carried out at the time of job applications.

– A similar screening process shall be carried out or incorporated as part of the contract for contractors and temporary staff in accordance with the Risk Assessment of the External Parties.

– Information systems technical details, such as network addresses, network diagrams, and security software employed, will not be revealed to job applicants until they have been hired and have signed a confidentiality agreement.

– Persons who have a criminal conviction will not be hired into, retained for, promoted into, or maintained in computer-related positions of trust.

5.1.3. Terms and conditions of employment

– The terms and conditions of employment will include the employee’s responsibilities for information security as laid down by the Information Security Policy.

– Employees of the Company will grant the Company exclusive rights to patents, copyrights, inventions, or other intellectual property they originate or develop.

5.2. During employment

5.2.1. Management responsibilities

– Management will require employees, contractors and third party users to apply security in accordance with Company’s established policies.

– Management will ensure that Function Heads are responsible for promoting security across their departments.
– Function Heads will ensure that information security within their departments is treated as mandatory and employees are encouraged to adhere to Company’s information security policies.

5.2.2. **Information security awareness, education, and training**

– All employees of the organisation and, where relevant, third-party users will receive appropriate training and regular updates in organisation policies and procedures.

5.2.3. **Disciplinary process**

– The violation of organisation security policies and procedures by employees will be dealt with rules and procedures of existing Oil Executives’ Conduct, Discipline and Appeal Rules and modified standing Order.

5.3. **Termination or change of employment**

5.3.1. **Termination responsibilities**

– Human Resources will notify IT department and all other stakeholders (from support and business functions) about the transfer or termination of any employee and any other third party personnel or contractors of the organization without delay.

– Unless the IT department has received instructions to the contrary, within 30 days after an employee has permanently left the Company, all files held in that user’s directories will be purged unless reporting manager needs that data.

– The system user IDs will be disabled for a period of one month after an employee has permanently left the Company

5.3.2. **Return of assets**

Company property including, but not limited to, portable computers, library books, documentation, building keys, magnetic access cards, etc. will be returned at the time when an employee leaves the organization. Employees shall also be mandated to get sign off from
the following department (but not limited to) on the no dues/clearance form after return of assets:

- IT
- Finance
- Administration
- Human Resources
- Legal

5.3.3. Removal of access rights

System privileges and access to information and information assets to an employee will be removed within 72 working hours after receiving mail from personnel department.

6. Physical and Environmental Security

Objective: To prevent unauthorized physical access, damage, and interference to the organization’s premises and information.

6.1. Secure areas

6.1.1. Physical security perimeter

- All multi-user computer and communications equipment will be located in a room with adequate access control mechanism installed e.g. keypad or a proximity cards access.
- Every Company multi-user computer and communications facilities will have a physical security plan that is reviewed and updated annually by the manager in charge of the facility.

6.1.2. Physical entry controls

- Access to every office, computer room, and work area containing sensitive information will be physically restricted to limit access to authorized personnel only.


**OIL-IS-POL-IS-1.0 (Information Security Policy)**

- All persons will wear an identification badge on their outer garments ensuring that both the picture, in case of employees, and information on the badge are clearly visible whenever they are in Company secure buildings or facilities.

- Employees will not permit unknown or unauthorized persons to pass through doors, gates, and other entrances to restricted areas at the same time when they go through these entrances.

- Visitor or other third-party access to Company offices, computer facilities, and other work areas containing sensitive information will be controlled by guards, receptionists, or other staff.

**6.1.3. Securing offices, rooms, and facilities**

- There will be no signs indicating the location of computer or communications centres.

- Multi-user computer and communications facilities (including telephone closets, network router and hub rooms, voice mail system rooms, and similar areas containing computer and / or communications equipment) will be kept locked at all times and not be accessible by visitors without an authorized IT staff escort to monitor all work being performed.

**6.1.4. Protecting against external and environmental threats**

- Multi-user computer and communications facilities will be located above the first floor in buildings, away from kitchens.

- Local management will provide and adequately maintain fire detection and suppression, power conditioning, air conditioning, humidity control, and other computing environment protection systems in every Company multi-user computer and communications facility.

- All openings to walls (such as doors and ventilation ducts) surrounding multi-user computer and communications facilities will be self-closing.
6.1.5. **Working in secure areas**

- The main multi-user computer and communications facility will be staffed at all times by technically-competent staff 24 hours a day, seven days a week, 365 days a year.
- Employees and visitors will not smoke in multi-user computer - and communications facilities.

6.1.6. **Public access, delivery, and loading areas**

- A secured intermediate holding area will be used for computer supplies, equipment, and other deliveries.

6.2. **Equipment security**

6.2.1. **Equipment sitting and protection**

- All elements of production computer systems including, but not limited to, servers, firewalls, hubs, routers, etc will be physically located within a secure area and labeled by using bar code.
- The physical address of every Company multi-user computer and communications facility is confidential and will not be disclosed to unauthorized individuals.
- Employees will not bring their own computers, computer peripherals, or computer software into Company facilities without prior authorization from their department head.

6.2.2. **Supporting utilities**

- All servers and network equipment will be fitted with uninterruptible power supply systems, electrical power filters, or surge suppressors that have been approved.
- All Company multi-user computer and communications facilities will have alternative source of power, such a Generator sets etc, so that normal business operations are sustainable even during extended period of unavailability of main power supply.
6.2.3. **Cabling security**

- Power and telecommunications cabling carrying data supporting information services will be protected from interception or damage.

- Cabling of Company’s internal network will be physically protected from any damage or vandalism by lying in plenum spaces.

6.2.4. **Equipment maintenance**

- Preventative maintenance will be regularly performed on all computer and communications systems.

- All information systems equipment used for production processing will be maintained in accordance with the supplier’s recommended service intervals and specifications, with any repairs and servicing performed only by qualified and authorized maintenance personnel.

- Hardware and software that is required to read data storage media held in the Company archives must be kept on-hand, properly configured, and maintained in operational condition.

- All hardware and software products will be registered with the appropriate vendors for maintenance, after Company staff takes delivery of new or upgraded information systems products.

- The Annual Maintenance Contracts for all hardware and software products, if applicable, will be monitored and reviewed after every six months.

6.2.5. **Security of equipment off-premises**

- Any use of equipment for information processing outside company premises will require authorization by management. Authorization for issue of mobile computing devices (laptops) will be considered as an authorization for use of equipment for information processing outside Company premises.
Employees will store mobile phones and other hardware sensibly and securely when storing outside Company’s premises e.g. hotels, airports. Equipment will not be left unlocked, logged in or powered up without the employee being with the equipment.

6.2.6. Secure disposal or re-use of equipment

– Information will be erased from equipment prior to disposal or re-use.
– Equipment will be disposed in an environmentally sensitive manner, taking account of any recycling facilities provided by manufacturers, local authorities or commercial organizations.

6.2.7. Removal of property

– Equipment, information or software belonging to the organization will not be removed without authorization of the relevant departmental manager.

7. Communications and Operations Management

Objective: To ensure the correct and secure operation of information processing facilities.

7.1. Operational procedures and responsibilities

7.1.1. Documented operating procedures

– Company IT department, after the approval from Chief Information Security Officer, may, at any time, alter the priority, or terminate the execution of any user process that is consuming excessive system resources or is significantly degrading system response time, after a prior authorization.
– Company IT department staff will terminate user sessions or connections if the usage is deemed to be in violation of security policy.
– At all times, at least two IT department personnel will be able to provide any given essential technical service (irrespective of the local/remote) for information systems critical to business during office hours.
The operating procedures will be documented, maintained, and made available to all users who need them and will include:

- backup procedure;
- incident management procedure;
- support contacts in the event of unexpected operational or technical difficulties;
- installing software and patches;
- job scheduling;
- system start-up and shutdown procedure; and
- management of audit-trail and system log information.

7.1.2. Change management

- All production computer and communications systems at the Company will employ a formal change management procedure to authorize all significant changes to software, hardware, communications networks, and related procedures.
- Changes to all information processing facilities and systems will be controlled and documented to ensure that any changes and additions do not compromise information security.
- All default privileged user IDs such as “administrator,” “auditor,” or “installer” will be disabled before any multi-user computer operating system is installed on Company systems.
- Extensions, modifications, or replacements to production operating system software will be made only after an approval from Change Advisory Board comprising of Change Manager and CISO.
– All operating system modules or utilities that are not used and are not necessary for the
operation of other essential systems software will be removed or otherwise disabled
prior to being used with production information.

– The details of all the changes approved and performed will be communicated to all the
relevant persons or departments.

7.1.3. Segregation of duties

– All the mutually exclusive roles and corresponding access permissions will be identified
and reviewed annually.

– Whenever a Company computer-based process involves sensitive information, the
system will include controls involving separation of duties or other compensating
control measures that ensure that no one individual has exclusive control over these
types of information assets.

7.1.4. Separation of development, test, and operational facilities

– Separate people will perform production application source code development and
maintenance, production application staging and operation, and production application
data manipulation.

– Production business application software in development will be kept strictly separate
from this same type of software in testing through physically separate computer
systems or separate directories or libraries with strictly enforced access controls.

– Employees who have been involved in the development of specific business application
software will not be involved in the formal testing or day-to-day production operation of
such software.
7.2. Third party service delivery management

7.2.1. Service delivery

– The Company will reserve the right to immediately terminate network connections with all third-party systems not meeting the information security requirements.

– Arrangements involving third-party access to Company internal systems will be agreed in a formal contract containing all necessary security requirements.

– Before third-party users are permitted to reach Company internal systems through computer connections, approval of the Chief Information Security Officer will be obtained. These third parties include information providers such as outsourcing organizations, business partners, contractors, and consultants working on special projects.

7.2.2. Monitoring and review of third party services

– All agreements with organizations providing services to the Information Security function will stipulate that the Company will have the right to audit the information security controls implemented.

7.2.3. Managing changes to third party services

– Third-party vendors will be given only in-bound connection privileges when the applicable system manager determines that they have a legitimate business need. These privileges will be enabled only for the time period required to accomplish previously-defined and approved tasks. Third-party vendor access that will last longer than one day must be approved by the CISO.

– Unless the relevant Information Owner has approved in advance, employees will not place anything other than Company public information in a directory, on a server, or in any other location where unknown parties could readily access it.
7.3. System planning and acceptance

7.3.1. Capacity management

– The use of computer and network resources will be monitored, tuned, and projections will be made for future capacity requirements to ensure the required system performance and to avoid misuse and excessive use of resources.

– Employees will not establish intranet servers, electronic bulletin boards, local area networks, modem connections to existing internal networks, or other multi-user systems for communicating information without the specific approval of CISO.

7.3.2. System acceptance

– Before computer systems and network segments can be connected to the Company network they will meet the security criteria established by ISWG including, but not limited to:
  
  o latest OS patches;
  
  o anti-virus with latest definition;
  
  o local admin password change; and
  
  o host name.

– All Company servers, hosts, firewalls, and other multi-user computers will be configured according to security requirements established by the ISWG.

– All in-house developed system will have adequate documentation prior to deploying the system.

– Before being used for production processing, new or substantially changed business application systems will be approved by the CAB which includes Change Manager and CISO and the respective user department.
The acceptance and sign-off of ISWG member, the involved user department, and the internal Audit department will be obtained before a program is granted production status on a multi-user computer.

All software that handles sensitive, critical, or valuable information, and that has been developed by end users, must have its controls approved by the ISWG member prior to being used for production processing.

7.4. Protection against malicious and mobile code

7.4.1. Controls against malicious code

Malicious software checking systems will run continuously on all personal computers, local area network servers, firewalls, and on electronic mail servers.

All files coming from external sources will be checked before execution or usage.

If users obtain malicious software alerts, they will immediately disconnect from all networks and cease further use of the affected computer, and call the Central Service Desk for technical assistance and will make no attempt to eradicate the virus.

All files containing software or executable statements will be verified to be virus free prior to being sent to any third party.

Before any files are restored to a production Company computer system from backup storage media, these will be scanned with the latest version of virus screening software.

Users will not intentionally write, generate, compile, copy, collect, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any Company computer or network.
**OIL-IS-POL-IS-1.0 (Information Security Policy)**

7.4.2. **Controls against mobile code**

- Employees will not enter into Internet processes that involve the use of mobile code, permit mobile code to execute on their machines, or permit the placement of mobile code on their machines.

7.5. **Back-up**

7.5.1. **Information back-up**

- Regular backups will be taken for all essential business information; a formal backup plan will be documented identifying the information systems, information to be backed up, type & frequency of backups.

- All backup activities will be logged through an audit trail.

- Information owners will provide the application specific backup requirements or data backup requirement to the IT department as and when required.

- Every user will back up the local data on their workstations and laptops on the network drive/shared folder.

7.5.2. **Information backup testing**

- The data and system files that are backed up will be tested only if no restoration request is received in once in entire month.

- Any discrepancies or errors found during the backup testing will be reported to the Information Owner concerned.

- The test results will be documented and the backup process will be modified to avoid similar discrepancies in future.

7.5.3. **On-site and off-site backups**

- On-site data backup will not be kept in unsecured location outside the server room.
Off-site data will be kept at offsite location in fireproof cabinet in the Head Office, Gurgaon.

7.5.4. **Security requirement for backup tapes in transit**

- Whilst the data is in transit, the same level of security will be applied for the data and system files as when they are on the servers.

7.5.5. **Labelling of backup tapes**

- The backup media will be labeled to a consistent standard and will comply with the information classification requirements.

7.5.6. **Information Restore**

- Written request with approval from the Information Owner will be given to IT department for backup restoration requirements.

- A log will be maintained showing details of the information restored, date, time and approval of the Information Owner.

7.6. **Network security management**

7.6.1. **Network controls**

- IT department will design Company communications networks so that no single point of failure could cause network services to be unavailable.

- All internal networks will be configured such that they can prevent or detect attempts to connect unauthorized computers.

- The network administrator will be alerted by the system if there is any possible breach of network security like unauthorized access, hacking or malicious software infection.

- Users will not test or attempt to compromise any information security mechanism unless specifically authorized to do so by the Chief Information Security Officer.
Users will not possess software or other tools that are designed to compromise information security.

Employees will not connect their own computers with Company computers or networks without prior authorization from their department head and the CISO. On receiving such approval on an exception basis, the connectivity would be provided only in the network segment logically isolated from the Company’s internal network.

Permission to connect other networks and computer systems in Company’s network will be approved by the CISO and be documented.

Employees and vendors working for the Company will not make arrangements for, or actually complete, the installation of voice or data lines with any carrier unless they have obtained written approval from the CISO.

All unused connections and network segments will be disconnected from active networks in public areas i.e. reception and lobby area.

The computer system or outside terminal accessing Company’s host system will adhere to the Company’s system security and access control guidelines.

The suitability of new hardware/software particularly the protocol compatibility will be assessed by the IT department before the connections are allowed to the Company’s network.

No Internet access will be allowed from database server/file server or any server hosting sensitive data.

Permission to install remote control communications software in Company’s network will be approved by the IT department/CISO, and documented.

Telephone numbers for dial-in devices will not be distributed to anyone other than people who have a demonstrated business need to use them.
7.6.2. Security of network services

- All web servers accessible through the Internet will be protected by a router or firewall approved by the ISWG member.
- Network services will only accept communications from authenticated sources.
- All connections between Company internal networks and the Internet or any other publicly-accessible computer network will include an approved firewall and related access control system.
- The privileges permitted through this firewall or related access control system will be based on business needs and will be defined in an access control standard issued by the ISWG member.
- Firewall configuration rules and permissible service rules will not be changed unless the permission of the CISO has been obtained.
- Wireless networks used for Company transmissions will always be configured to employ appropriately configured encryption.
- Wireless network gateways will always be configured so that they employ firewalls to filter communications with remote devices.
- Wireless technology will never be used for the transmission of unencrypted Sensitive information.

7.7. Media handling

7.7.1. Management of removable media

- Company employees will not store Sensitive information with non-sensitive information on any removable data storage media unless authorized by the Information owner.

7.7.2. Disposal of media

- Computer media will be disposed of securely and safely when no longer required.
7.7.3. **Information handling procedures**

- Procedures will be defined for handling and storing information in order to protect the information from unauthorized disclosure or misuse.

7.7.4. **Security of system documentation**

- Prior to being released to third parties, all documentation that describes Company information systems or systems procedures will be reviewed.
- All Company computers related documentation is sensitive, and will not be taken elsewhere when an employee leaves the employment of the Company.

7.8. **Exchange of information**

7.8.1. **Information exchange policies and procedures**

- All inquiries made by external agencies or personnel will be diverted to the Public Relations or to the designated spokespersons.
- All employees will take all possible care to avoid information disclosure while discussing Company information in public places such as in building lobbies or on public transportation.
- All employees who will be delivering speeches, writing papers, or otherwise disclosing information about the Company or its business will obtain pre-authorization from the Corporate Communications department.
If Sensitive information is discussed verbally in a meeting, seminar, lecture, or related presentation, the speaker will clearly communicate the sensitivity of the information and remind the audience to use discretion when disclosing it to others.

After each meeting is over, all erasable surfaces in conference rooms including, but not limited to, black boards and white boards will be erased.

Company video conferencing sessions will not be recorded unless this recording is approved in advance by the IS department and communicated in advance to all video conference participants.

### 7.8.2. Exchange agreements

- Exchanges of in-house software or internal information between the Company and any third party will be accompanied by a written agreement that specifies the terms of the exchange, and the manner in which the software or information is to be handled and protected.

- Before employees release any Sensitive Company information, or enter into any contracts, the identity of the individuals and organizations contacted will be confirmed through digital certificates, letters of credit, third-party references, or telephone conversations.

### 7.8.3. Physical media in transit

- Employees will not travel on public transportation when physically in possession of Sensitive Company information unless specific management approval has been obtained.

- Whenever a hardcopy version of Sensitive information is removed from Company premises, it will not be left unattended in a motor vehicle, hotel room, office, or some other location, even if the vehicle or room is locked.
7.8.4. **Electronic messaging**

- Company system administrators will maintain electronic mail messages and accompanying logs as per backup management procedure.
- Employees will not employ any electronic mail addresses other than official Company electronic mail addresses for all company business matters.
- Unless the Information Owner or originator agrees in advance, or unless the information is clearly public in nature, employees will not forward electronic mail to any address outside of the Company network.
- Employees will not create and send, or forward externally-provided electronic mail messages that may be considered to be harassment or that may contribute to a hostile work environment.
- An electronic mail message will be retained for future reference if it contains information relevant to the completion of a business transaction, contains potentially important reference information, or has value as evidence of a Company management decision.
- Employees will not monitor electronic mail systems for internal policy compliance, suspected criminal activity, and other systems management reasons unless electronic mail monitoring tasks have been specifically delegated and approved by the Function Heads and Human Resources.
- Employees will not send or forward any messages through Company information systems that may be considered defamatory, harassing, or explicitly sexual, or would likely offend someone on the basis of race, gender, national origin, sexual orientation, religion, political beliefs, or disability.
- Employees will not use Company computer systems for the transmission of any type of unsolicited bulk electronic mail advertisements or commercial messages that are likely to trigger complaints from the recipients.
When employees receive unwanted and unsolicited electronic mail, they will forward the message to the electronic mail administrator and will not respond directly to the sender.

Users who receive an unexpected attachment to an electronic mail message that does not have a credible business-related explanation will not open the attachment until they obtain an explanation from the sender.

**7.8.5. Internet Usage Policy**

Internet access will be provided to the users for carrying out business activities in a secure manner. All the users will be uniquely identified and authenticated before being allowed to access the Internet. All activities performed under a user’s identification code will be identifiable and users shall be accountable for any activities performed using their identification code.

Connections from network to Internet will be only made through systems approved by the CISO and shall incorporate approved vendor provided security patches.

All web browsers will be configured to use CISO approved secure gateway HTTP proxy. These systems must, at a minimum, prevent all services except those that are explicitly allowed and have the capacity to be actively monitored and logged.

Access level will be defined for all the users based on the business requirements.

The Internet traffic content will be screened and access to web sites relevant for business information shall be allowed to the users.

Users will be restricted from accessing the web based e-mail sites, use of instant messengers, downloading of screensavers, trial version of software applications and other web sites that are not required for business purposes.

All access to the Internet will be logged and monitored. The management retains the right to inspect any and all files stored on or transmitted over its network assets.
(including but not limited to, local storage media, memory and mail files) for the purpose of investigating suspected violations of its business policies or non-compliance with local regulations.

- Users will not attempt to probe other systems in the external world for security weaknesses, compromise other systems, possess or transfer data illegally, or send offensive or abusive messages. They will not claim to represent on the Internet unless authorized to do so by the management.

7.8.6. **Business information systems**

- Users will not install new or upgraded programs on their workstations or personal computers and instead rely on IT department configured automatic network downloads for this maintenance.

- Private and Sensitive information will be shipped or sent through internal or external mails in a sealed opaque envelope marked “To Be Opened by Addressee Only”.

- If Sensitive information is to be sent by fax, the recipient will be notified of the time when it will be transmitted, and an authorized person will be present at the destination machine when the material is sent unless the fax machine is restricted such that persons who are not authorized to see the material being faxed may not enter.

- When sensitive information must be faxed, a cover sheet will be sent and acknowledged by the recipient, after which the sensitive information may be sent through a second call.

- Employees will not store Sensitive information on personal computer or workstation hard disk drives unless ISWG member has determined that adequate information security measures are employed.

- Office computer equipment will not be moved or relocated without the prior approval of the involved department manager.
7.9. Electronic commerce services

7.9.1. Publicly available information

- Every public written use of the Company name in published material will require the advance approval of a Company Director or the Corporate Communications department.

- Employees will not misrepresent, obscure, suppress, or replace their identity on any electronic communications.

- Unofficial comments that users post to an electronic mail system, an electronic bulletin board system, or other electronic systems will not be considered as formal statements of or the official position of the Company and will not be made from Company systems.

7.10. Monitoring

7.10.1. Audit logging

- All production application systems that handle sensitive Company information will generate logs that capture every addition, modification, and deletion to such sensitive information.

- Computer systems handling sensitive, valuable, or critical information will securely log all significant security relevant events including, but not limited to, password guessing attempts, attempts to use privileges that are not authorized, modifications to production application software, and to system software.

- All unsuccessful and non authorized logon attempts to connect to Company production information systems will be logged.

7.10.2. Monitoring system use

- All user activity is subject to logging and possibly subsequent analysis.
Users will not perform any activity on Company information systems that could damage the reputation of the Company. Unbecoming conduct could lead to disciplinary action including revocation of access control privileges.

7.10.3. Protection of log information

- Audit logs recording exceptions and other security relevant events will be produced and kept securely for one year to assist in future investigations and access control monitoring.

- Computerized logs containing security relevant events will be retained for at least three months, during which time they must be secured such that they cannot be modified, and such that they can be read only by authorized persons.

7.10.4. Administrator and operator logs

- All Company multi-user production systems must have computer operator logs that show:
  
  o  Login failures;
  
  o  Account lockouts;
  
  o  System boot and restart times;
  
  o  System or application start, stop, re-initialization (with user identity and time of action);
  
  o  System configuration changes;
  
  o  System errors and corrective actions taken; and
  
  o  Production applications start and stop times.

7.10.5. Fault logging

- A formal problem management procedure will be in place to record the security problems, reduce their incidence, and to prevent their recurrence.
7.10.6. Clock synchronization

- All multi-user computers connected to the Company internal network will always have the current time accurately reflected in their internal clocks.

8. Access Control

Objective: To control access to information.

8.1. Business requirement for access control

8.1.1. Access control policy

- The Company will ensure that access to its information and business processes is controlled as per the business and security requirements.

- Access to Public and Internal Use Only information will not be restricted with access controls that discriminate by specific user. For example, Public information is available at the Company web site, and Internal Use Only information is available on the Company intranet.

- Access to Sensitive information will be granted only when a legitimate business need has been demonstrated and access has been approved in advance by the Information Owner.

- Users will be responsible for all activity that takes place with their user ID and password or other authentication mechanism.

- A user will change their password immediately if they suspect that it has been discovered or used by another person and report this to the IT Help Desk.

- Employees will not use Company information systems to engage in hacking activities that include, but are not limited to, gaining unauthorized access to any other information systems damaging, altering, or disrupting the operations of any other
information systems and capturing or otherwise obtaining passwords, encryption keys, or any other access control mechanism that could permit unauthorized access.

– Employees will not move information classified at a certain sensitivity level to a less sensitive level unless this action is a formal part of an approved declassification process.

– File access control permissions for all Company networked systems will be set to a default that blocks access by unauthorized users.

**User access management**

8.1.2. User registration

– All user IDs on Company computers and networks will be constructed according to the Company standard user ID construction, must clearly indicate the responsible individual’s name, and under no circumstances are such user IDs will be permitted to be generic, descriptive of an organizational title or role, descriptive of a project, or anonymous.

– Every user will have a single unique user ID and a personal secret password for access to the Company multi-user computers and computer networks.

– There will be a formal user access creation and deletion procedure for granting access to all multi-user information systems and services.

– User creation/ modification request will be required to be authorized by the line manager and submitted to Application Owner before user access is created.

8.1.3. Privilege Management of employees

– An employee’s manager will initiate the access control approval process, and the privileges granted will remain in effect until the employee’s job changes or the employee leaves Company. If either of these two events occurs, the manager will notify the IT department immediately.
The computer and communications system privileges of all users, systems, and programs will be restricted based on the need to know.

By default, all users will be granted basic information systems services such as electronic mail, intranet and word processing facilities etc.

All other system capabilities will be provided through job profiles or by special request approved by the involved Application Owner.

Employees who are assigned high level privileges will use a different login for normal business use (e.g. “System Administration” login must not be used for checking e-mail).

Privileges will be granted on the server after adequate approval from the manager and CISO.

The privileges associated with each application as well as the role to which they need to be allocated will be identified and documented.

8.1.4. Privilege Management of non-employees

All non-employees, contractors, consultants, temporaries, and outsourcing organizations will also go through a similar access control request and authorization procedure which will be initiated by the project manager or relevant departmental manager.

The privileges to these non-employees will be revoked immediately by the IT department when the project is complete, or when the non-employees stop working with the Company.

Every user ID established for a non-employee will have a specified expiration date.

The relevant project manager or relevant departmental manager will review the need for the continuing privileges of non-employees every quarter.

8.1.5. User password management

User-chosen fixed passwords will not be reused or recycled for at least last 5 passwords.
OIL-IS-POL-IS-1.0 (Information Security Policy)

- All Company computer systems that employ fixed passwords at log on will be configured to permit only five attempts to enter a correct password, five unsuccessful attempts will lock the account. A root cause should be done to find the cause of lock out.

8.1.6. Review of user access rights

- All user IDs will automatically have the associated privileges revoked after a 60-day period of inactivity.
- The system access history and user logs will be reviewed periodically by the IT department. Redundant and unused user accounts will be removed on a quarterly basis.
- Management will conduct a formal review of users’ access rights twice in a year.

8.2. User responsibilities

8.2.1. Password use

- Users will not employ any password structure or characteristic that results in a password that is predictable or easily guessed including, but not limited to, words in a dictionary, derivatives of user IDs, common character sequences, personal details, or any part of speech.
- Passwords will never be shared or revealed to anyone other than the authorized user.
- Users will not store fixed passwords in any computer files, such as logon scripts or computer programs, unless the passwords have been encrypted with authorized encryption software.
- Passwords will not be written down unless a transformation process has concealed them, or they are physically secured, such as placed in a locked file cabinet.

8.2.2. Unattended user equipment

- Personal computers, computer terminals and printers should be left logged off or protected with a screen and keyboard locking mechanism controlled by a password, token or similar
user authentication mechanism when unattended and will be protected by key locks, passwords and other controls when not in use.

8.2.3. **Clear desk and clear screen policy**

- Oil India will have a clear desk and a clear screen policy aimed at reducing the risks of unauthorized access, loss of, and damage to information.

- Outside of regular working hours, all employees will clear their desks and working areas from all sensitive or valuable data.

- When not in use, sensitive information left in an unattended room will be locked away in appropriate containers.

8.3. **Network access control**

8.3.1. **Policy on use of network services**

- Users will only have direct access to the services that they have been specifically authorized to use.

- Users will not establish any external network connections that could permit third party users to gain access to Company systems and information, unless prior approval from ISWG department has been obtained.

- When using Company information systems, or when conducting Company business, users will not deliberately conceal or misrepresent their network identity.

8.3.2. **User authentication for external connections**

- All users remotely accessing the Company computer and networks will ensure that they are authenticated through SSL Gateway prior to accessing organization network/ systems.

- Access control mechanism will be deployed to prevent unauthorized access to Company computer and information systems.
Inbound connection to Company computers or networks through an office desktop modem will be prohibited unless specific approval has been obtained from the ISWG member.

Outbound connection to third-party networks including the Internet through office desktop modems or other types of modems will be approved by the ISWG member.

Leaving personal computer-linked modems in auto-answer mode will be prohibited unless a remote user identification system approved by the IS department is installed.

### 8.3.3. Equipment identification in networks

- Automatic terminal identification will be considered to authenticate connections to specific locations and also to authenticate portable equipments.
- When terminal identification is used to authenticate a terminal connection to a specific location, the physical access to the terminal will be restricted to the authorized employees only.

### 8.3.4. Remote diagnostic and configuration port protection

- Access to all diagnostic ports will be provided after approval from Chief Information Security Officer. Connection to the remote diagnostic ports will be provided using secure communication channels.

### 8.3.5. Segregation in networks

- Every sensitive and high-reliability system managed by or owned by the Company will have its own dedicated computers and networks, unless approved in advance by the CISO.

### 8.3.6. Network connection control

- All Company internal network devices including, but not limited to, routers, firewalls, and access control servers, will have unique passwords or other access control mechanisms.
- Unattended active internal network ports that connect to the Company internal computer network will not be placed in public areas including, but not limited to, building lobbies.
8.3.7. Network routing control

– All Company internal networks will be divided into security zones wherever appropriate.

– All Company internal networks will have routing controls to ensure that computer connections and information flows do not breach the access control policy of the business applications.

8.4. Operating system access control

8.4.1. Secure log-on procedures

– The system shutdown option which allows users to shutdown the system without logging in first, will be restricted on all servers housing Sensitive information.

– When logging into a Company computer or data communications system, if any part of the logon sequence is incorrect, the user will be given only feedback that the entire logon process was incorrect.

– The number of unsuccessful logon attempts will be limited to five after which the system will lock that particular User ID. All unsuccessful login attempts will be recorded.

– On completion of a successful log-on the following information will be logged:
  
  o Date and time of the previous successful log-on;
  
  o Details of any unsuccessful log-on attempts since the last successful log-on.

– A greeting on any external network connection will not be displayed until the user is authenticated through a sign-on sequence that requires a unique user ID and password.
A message will be displayed on all network connections warning potential users that unauthorized use is prohibited and that legal action will be taken against offenders. (e.g., unauthorized access to the network is prohibited and illegal).

**8.4.2. User identification and authentication**

- A unique user ID will be created for any new Information System access request based on their stated business needs and security constraints.
- IT Help Desk personnel will never obtain user’s password to do their job. They will have all the privileges they require to do their job.
- User IDs will be linked to specific people and will not be associated with computer terminals, departments, or job titles unless authorized.

**8.4.3. Password management system**

- Where systems support it, fixed passwords will be required to change every 60 days and passwords will be changed the first time they are used.
- All fixed passwords will be at least 8 characters, and this minimum length will be enforced automatically where systems support it.
- All fixed passwords will include both alphabetic and numeric characters.
- All fixed passwords set by default by the hardware or software vendor will be changed before the involved system can be used for Company business activities.

**8.4.4. Use of system utilities**

- Access to local system control utilities (e.g., Batch Files, Unix Scripts etc.) will be restricted and controlled.
- These system utilities will be installed on local PCs and will be intended for use by IT to assist in resolving problems.
- Access to the system utilities must be limited to IT personnel only.
Remote control utilities for Central Service Desk personnel will only be used after the service desk has informed the user of this capability and has received permission from the user to use them.

Access to diagnostic test hardware and software will be strictly controlled and will be used only by authorized personnel for testing, trouble-shooting, and development purposes.

**8.4.5. Session time-out**

- Sessions on inactive terminals in high risk locations or serving high risk systems will time out after a defined period of inactivity to prevent access by unauthorized persons.
- After a period of 5 minutes of no activity online sessions with multi-user machines will be terminated automatically.

**8.5. Application and information access control**

**8.5.1. Information access restriction**

- All computer-resident information that is sensitive, critical, or valuable will have system access controls to ensure that it is not improperly disclosed, modified, deleted, or rendered unavailable.
- Access will be restricted for programs or system utilities that can dynamically alter data (e.g., programs that circumvent the standard logical access to data files) to those people who demonstrate a business need.
- User privileges will be defined such that ordinary users cannot gain access to, or otherwise interfere with, either the individual activities or the private data of other users.
- Systems logs or application audit trails will be disclosed only to the authorized to any person outside the team of individuals who ordinarily view such information to perform their jobs or investigate information security incidents.
8.5.2. **Sensitive system isolation**

- Sensitive systems will have a dedicated (isolated) computing environment, either logically or physically, including controlled access to utilities and program files.

- Direct physical or logical access to a database must be authorised by the Chief Information Security Officer.

8.6. **Mobile computing**

8.6.1. **Mobile computing and communications**

- Users will not store passwords, user IDs, or any other access information in portable or remote systems.

- Users will be careful not to discuss sensitive information when in public places like hotel lobbies, restaurants, and elevators etc.

- Viewing sensitive information on a computer screen or hardcopy report will be prohibited when a user is in a public place such as seated on an airplane.

- Users will not provide sensitive information in voice mail messages or alphanumeric messages.

- When using public Internet terminals to check email, users will log out correctly from Company systems when finished.

9. **Information Systems Acquisition, Development and Maintenance**

**Objective:** To ensure that security is an integral part of information systems.
9.1. Security requirements of information systems

9.1.1. Security requirements analysis and specification

– Before a new system is developed or acquired, management of the user department will clearly specify the relevant security requirements.

– Business requirements for new systems or enhancements to existing systems will specify the required security controls.

– All software developed in-house to process sensitive, valuable, or critical information such as production systems, will have a written formal specification that is part of an agreement between the involved Information Owner and the system developer, and drafted and approved.

– All software developed in-house that runs on production systems will be developed according to the Software Development Lifecycle (SDLC).

– SDLC will ensure that the software is adequately documented and tested before it is used for critical Company information.

– Where resources permit, there will be a separation between the production, development, and test environments.

– All production software testing will proceed with sanitized information where sensitive information is replaced with dummy data.

– Both users and programmers must never embed user IDs, readable passwords, encryption keys, or other security parameters in any file.
9.2. Correct processing in applications

9.2.1. Input data validation

– The system acquisition/development methodology of the Company will ensure that appropriate input data validation controls are existing/built-in the systems, prior to their deployment in the production environment.

9.2.2. Control of internal processing

– Company production systems will be built so that all the critical transactions processed will have a maker who processes the transactions and a checker who validates the transactions before executing it.

– Privileges will be established such that system users are not able to modify information data in an unrestricted manner.

– All the critical transactions will be logged and reviewed periodically based on the criticality involved.

9.2.3. Message integrity

– Input to production computer systems submitted for processing will be designed post approval.

9.2.4. Output data validation

– Data output from an application system will be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.

9.3. Cryptographic controls

9.3.1. Policy on the use of cryptographic controls

– Encryption processes will not be used for Company information unless the processes are approved by the Chief Information Security Officer.
– Encryption will be adopted for information assets based on the criticality of information. Standard encryption technology would be deployed for encryption unless required by regulatory requirements.

– Users will not employ encryption, digital signatures, or digital certificates for any business activity or business information without the written authorization of their department manager, the completion of proper training and having their systems configured by authorized personnel.

– Employees will never employ encryption utilities requiring a user to input a password or encryption key.

9.3.2. Key management

– A key management system based on an agreed set of standards will be used to support the use of cryptographic techniques.

9.4. Security of system files

9.4.1. Control of operational software

– Users will not write production computer programs unless specifically authorized by the CISO.

– All security fixes provided by software vendors and identified for implementation will go through the Change Management Procedure.

– Software requirements for any department will have an appropriate business case and budget approvals from the business department and will obtain a technical clearance from the IT department before deployment in the production system.

– IT department will be exclusively responsible for installing and supporting software on company computers for:
  
  o Office desktop computers (Local and Remote Locations);
OIL-IS-POL-IS-1.0 (Information Security Policy)

- Company computers systems (Local and Remote Locations); and
- Servers (Local and Remote Locations).

- Users will not install new or upgraded operating systems or application software on personal computers or other machines used to process Company information.

- Employees requiring software not published in the standard software list must request such software from the IT department after adequate approvals from the Line Manager.

- Unauthorised software including freeware and demo copies of software will not be installed on Company’s systems without written permission from the IT department.

9.4.2. Protection of system test data

- Unless written permission is obtained from the IT department, all software testing for systems designed to handle private information will be accomplished with production information that no longer contains specific details that might be valuable, critical, sensitive, or private.

- Where access to production business information is required so that new or modified business application systems may be developed or tested, only “read” and “copy” access will be granted on production machines for the duration of the testing and related development efforts, and will be promptly revoked upon the successful completion of these efforts. This will be approved by the IT department and the Business functions.

9.4.3. Access control to program source code

- Computer operations staff will not be given any access to information data, production programs, or the operating system beyond that which they need to perform their jobs.
9.5. Security in development and support processes

9.5.1. Change control procedures

– Business application software in development will be kept strictly separate from production application software through physically separate computer systems or separate directories or libraries with strictly enforced access controls.

– Documentation reflecting the nature, approval and performance of all significant changes to production computer and communications systems owned by the Company will be prepared and approved before the change takes place.

– Management will ensure that all software development and software maintenance activities performed by in-house staff subscribe to Company policies, standards, procedures, and systems development conventions.

– All production system software that is migrated into production will be authorized by IT department.

– Every non-emergency change to production systems will be shown to be consistent with the information security architecture and approved by management as part of the formal change control procedure.

9.5.2. Technical review of applications after operating system changes

– IT department will configure production servers with those operating systems that permit unwanted or unneeded functionality to be completely removed.

– All Company networked production systems will be adequately-staffed for expediently and regularly reviewing and installing all newly released systems software patches, bug fixes, and upgrades online with the host hardening checklist.
9.5.3. Restrictions on changes to software packages

– Prior to being installed, new or different versions of the operating system and related systems software for multi-user production computers will go through the established change management procedure.

9.5.4. Information leakage

– Where sensitive information is involved, the Company will procure software only from reputable vendors. Additionally, to identify Trojan horses or other malicious code, procurement of source code along with the software and inspection of the same may be considered.

9.5.5. Outsourced software development

– Third parties who develop software for the Company will be bound by a contract.

9.6. Technical vulnerability management

9.6.1. Control of technical vulnerabilities

– The IT department will be responsible for the technical vulnerability management including vulnerability monitoring, vulnerability risk assessment, patching and asset tracking.

– Before installing patches, the risks associated with installing the patch will be assessed.

– Patches for production information systems will be tested and evaluated before they are installed to ensure they are effective and do not result in side effects that cannot be tolerated.

10. Information Security Incident Management

Objective: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.
10.1. Reporting information security events and weaknesses

10.1.1. Reporting information security events

– IT department will establish a framework for reporting, responding to an escalating information security events configure the same in the incident management system.

– All employees, contractors and third party users will be responsible for reporting all identified security events and incidents promptly.

10.1.2. Reporting security weaknesses

– IT department will establish an incident management procedure for reporting, responding to an escalating any suspected security weakness or threat to systems or services.

– Users will report all information security alerts, warnings and suspected vulnerabilities to the management, in a timely manner, and will share such information with only with authorized personnel.

– Employees will promptly notify management of all conditions that could lead to a disruption of business activities.

10.2. Management of information security incidents and improvements

10.2.1. Responsibilities and procedures

– Management will establish a procedure to ensure an effective, timely and orderly response to information security incidents. Guidelines will be established for collective and maintaining evidences collected as required by legislation.

10.2.2. Learning from information security incidents

– Information security incidents will be monitored and analysed on weekly basis.

– Incidents with high business impact will be identified and appropriate controls will be enhanced to reduce the risk from future occurrences of such incidents.
10.2.3. Collection of evidence

- Where action against a person or organization involves the law, either civil or criminal, the evidence collection and presentation will conform to applicable laws. This will include compliance with any published standard or code of practice for the production of admissible evidence.
- All investigations of alleged criminal or abusive conduct will be treated as restricted information to preserve the reputation of the suspected party until charges are formalized or disciplinary action taken.
- All internal investigations of information security incidents, violations, and problems, will be conducted by staff authorized.


Objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

11.1. Information security aspects of business continuity management

11.1.1. Including information security in the business continuity management process

- Business process owners will be responsible for ensuring that the key events that can cause disruption to their processes are identified and their potential adverse impact, financial & non-financial, is documented.
- The scope of the Business Continuity Plan will take into account applicable factors including customer requirements and legal regulations. The following will be considered while implementing any DR / BCP program:
  - identify critical business functions, applications and supporting technologies;
  - develop an appropriate cost effective recovery strategy;
OIL-IS-POL-IS-1.0 (Information Security Policy)

- identify alternate, backup locations with the necessary infrastructure to support the recovery needs;
- identify the management and membership of the disaster response and recovery teams;
- identify and document the required recovery actions, identify and ensure the availability of required resources, and compile this information as the recovery plan;
- train the recovery teams in the performance of their specific tasks;
- identify vendor recovery support capability;
- identify data protection and data recoverability status;
- identify functional team, recovery support and response capabilities; and
- develop an ongoing testing and maintenance program to ensure that all processes are in a constant state of recovery readiness.

11.1.2. Business continuity and risk assessment

- A strategy plan, based on appropriate risk assessment, will be developed for the overall approach to business continuity. Key considerations in such a plan will be:
  - identify events that cause interruptions to business processes; and
  - consider all critical business processes, not just information processing facilities.

11.1.3. Developing and implementing continuity plans including information security

- All departments will establish and use a logical framework for classifying all information resources by recovery priority that will permit the most critical information resources to be recovered first.
OIL-IS-POL-IS-1.0 (Information Security Policy)

- All departments will prepare, periodically update and regularly test the business recovery plan that specifies how alternative facilities will be provided so employees can continue operations in the event of a business interruption.

11.1.4. Business continuity planning framework

- A single framework of business continuity plans will be maintained to ensure that all plans are consistent, and to identify priorities for testing and maintenance.

11.1.5. Testing, maintaining and re-assessing business continuity plans

- If critical business activities could reasonably be performed with manual procedures rather than computers, a manual computer contingency plan will be developed, tested, periodically updated, and integrated into computer and communication system contingency plans.

- Oil India management will annually revise and document the support levels that will be provided in the event of a disaster or emergency.

- Computer and communication system contingency plans will be routinely tested and followed up with a brief report to top management detailing the results.

- Each calendar quarter, emergency contact information will be validated and revised indicating for every employee involved in business continuity and disaster recovery planning and implementation.

- The roles and responsibilities for both information systems contingency planning and information systems recovery will be reviewed and updated annually.

12. Compliance

Objective: To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements as defined by organization’s policy, procedure, standard or guideline.
12.1. Compliance with legal requirements

12.1.1. Identification of applicable legislation

- All relevant statutory, regulatory and contractual requirements will be defined explicitly and documented for all information processing facilities.

12.1.2. Intellectual property rights (IPR)

- The Company will be the legal owner of all business information stored on or passing through its systems, except the information clearly owned by third parties.

- All intellectual property, such as patents, copyrights, inventions, etc., developed by a user while employed by the Company, will be the property of the Company.

- At the time of termination of their relationship with the Company, all employees will return any intellectual property provided or developed during the period of the person’s employment.

- All Company intellectual property will be classified as per the Company’s data classification policy and labelled and handled as per Company policies.

- Software and hardware will be used in compliance with all legal, statutory, regulatory and contractual compliance and after due authorization.

- Software, licensed to the Company, will only be deployed and used on Company owned information processing facilities.

- Unless otherwise provided in the applicable license, notice, or agreement, copyrighted software will not be duplicated, except for back up and archival purposes.

- The IT Manager will be the custodian of the original copies of all Company hardware and software licenses.

- Any software that is acquired illegally or does not have a valid license will not be deployed or used on Oil India information processing facilities.
– Internal Audit department will conduct audit for license compliance every 12 months.

– Users will not copy, or reproduce in any way, copyrighted material from the Internet on information systems.

12.1.3. Protection of organizational records

– Oil India will manage the lifecycle of all records created or received by it in pursuance of legal obligations or transactions of business.

– All company records and information, such as personnel details, legal documents, will be retained and disposed off only in accordance with the retention periods as per the applicable laws.

– All restricted and confidential information will be destroyed in secure manner.

12.1.4. Data protection and privacy of personal information

– Oil India will implement controls for collecting, processing, and disseminating personal information. Employee personal data maintained on information systems will be secured through implementation of appropriate security controls.

– Only select authorized personnel will have access to such information. The security controls will address:

  o Mechanisms for ensuring that information is obtained and processed fairly, lawfully and properly.

  o Ensuring that information is accurate, complete and up-to-date, adequate and relevant.

  o Appropriate weeding and deletion of information.

  o Compliance with individual’s rights, such as subject access.

  o Compliance with the relevant data protection/ privacy regulations. Legal team will be responsible for identifying and marinating a list of applicable data
protection/privacy regulations and the same will be communicated to the CISO on a continuous basis.

- Contracts with third parties handling personal information will include clauses on right to audit.
- Oil India may log, review, and utilize any personal information stored on or passing through its systems.
- Oil India will, at its discretion, monitor usage of its information assets as per applicable laws and terms and condition of employment agreed upon by the Company and the employee. This may include logging and reviewing of user activity such as telephone numbers dialled, web sites visited from Oil India owned assets, electronic communications exchanged through Company information processing facilities etc.

12.1.5. Prevention of misuse of information processing facilities

- Oil India information systems will be used only after authorization from management and for business purposes only.
- Oil India will not be responsible for the safe keeping of any personal data on its systems.
- Users of Oil India assets will not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate or compromise information systems security, unless specifically authorized by the IS department.

12.2. Compliance with security policies and standards, and technical compliance

12.2.1. Compliance with security policies and standards

- Management of the IT department/IA will prepare an annual plan to ensure its computer and communications systems are compliant with this policy.
- The CISO will ensure that all security procedures within her/his area of responsibility are carried out correctly and within the Information Security Management Structure framework.
In support of the review, all areas should be considered for regular review to ensure compliance with security policies and standards.

12.2.2. Technical compliance checking

– Internal Audit management must perform an annual review and random tests of production computer system backup processes.

– Technical compliance check will be regularly carried out, which involves examination of operational systems to ensure that hardware and software controls have been correctly implemented.

– ISWG will develop and execute compliance review plan based on risk assessment. The plan will define scope and frequency of review based on the business impact of the system.

– In addition to regular updates, information systems security risk assessments for critical information systems and critical production applications will be reviewed at least once every year, and all major enhancements, upgrades, conversions, and related changes associated with these systems or applications will be preceded by a risk assessment.

12.3. Information systems audit considerations

12.3.1. Information systems audit controls

– Internal Audit will review the adequacy of information system controls and compliance with such controls annually.

– Internal Audit will conduct annual compliance checks related to this information security policy.

– Audits of operational systems will be planned with due care and agreed upon by the business owner to minimize the risk of disruptions to business processes.
12.3.2. Protection of information systems audit tools

– Programming source code and its related technical analyses used to compromise security will be disclosed only to authorised personnel with a justifiable business requirement.

– All information assets directly connected to the Internet must be subjected to periodic risk assessment performed.

13. Non Compliance

– Failure to comply with the Information Security Policy may, at the full discretion of the Oil India, result in disciplinary action.
Document Details

<table>
<thead>
<tr>
<th>Title</th>
<th>ISMS Scope Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>1.0</td>
</tr>
<tr>
<td>Classification</td>
<td>Internal</td>
</tr>
<tr>
<td>Release Date</td>
<td>01.06.2013</td>
</tr>
<tr>
<td>Description</td>
<td>This document defines the scope of the ISMS implementation at OIL</td>
</tr>
<tr>
<td>Review Date</td>
<td>01.06.2013</td>
</tr>
<tr>
<td>Author</td>
<td>CISO</td>
</tr>
<tr>
<td>Reviewer/Custodian</td>
<td>CISO</td>
</tr>
<tr>
<td>Approved By</td>
<td>Information Security Council (ISC)</td>
</tr>
<tr>
<td>Owner</td>
<td>CISO</td>
</tr>
</tbody>
</table>

Distribution List

<table>
<thead>
<tr>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Distribution Only</td>
</tr>
</tbody>
</table>

Version History

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Version Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>01.06.2013</td>
</tr>
</tbody>
</table>
# Table of Contents

1. Purpose .................................................................................................................. 4  
2. Introduction ........................................................................................................... 4  
   2.1 Company Profile ............................................................................................... 4  
   2.2 Key Business Assets ......................................................................................... 4  
3. OIL’s Approach to information security management ........................................... 5  
4. Scope Definition Process ....................................................................................... 6  
   4.1 Business Understanding .................................................................................... 7  
5. Scope of ISMS .......................................................................................................... 8  

1 Purpose

This document presents the details of the scope of Information Security Management System (ISMS) defined for OIL (referred to as OIL/Company).

2 Introduction

2.1 Company Profile

Oil India Limited (hereafter referred as OIL), a premier National Oil Company, is engaged in the business of Exploration, Production and Transportation of Crude Oil and Natural Gas from defined concessional areas in Upper Assam and Arunachal Pradesh and parts of eastern, northern and western India. Oil India Private Limited was incorporated on 18th February 1959 as a partnership venture between the Government of India and the BOC for the management of Nahorkatiya and Moran discoveries. On 14 October 1981 Oil India became wholly owned Government of India enterprise. Oil operates in India from its offices locations in Upper Assam, Arunachal Pradesh and parts of eastern, northern and western India.

2.2 Key Business Assets

As part of its core business processes, Oil India Limited handles enormous volumes of geophysical and seismic data, drilling data, analytical data, production data, supply data and other business operational data including the employee data. Handling of information and data is in many forms, and includes storing, processing, transmitting, etc. Oil India Limited has also developed and implemented various software applications in the provision of its services to clients.

These enormous volumes of data are being maintained, processed and stored with the help of computer systems. Till the beginning of 2005 the data was stored/processed on legacy systems. In the year 2005, many of the business/operational processes are migrated to a high-tech ERP system on SAP suite of applications running on various operating system platforms like AIX, Sun Solaris and Windows 2003 Server. Also, in the same year core technical asset data
including geophysical, geological, reservoir, drilling and production data were converted from different legacy formats to industry standard digital data format and stored on a central repository under the E&P Databank Project implemented through M/s Landmark Graphics Corporation, now part of Halliburton Group. However, other business non-critical data (e.g. Library & Club) are continued to be processed on legacy systems. All the locations of Oil India are networked and are connected to the ERP system Servers at Duliajan through MPLS or VSAT or Fiber or Radio connectivity. OIL has a full-fledged IT department who maintains and supports the IT systems at Duliajan and other locations.

As the custodian of a large volume of information that is sensitive from commercial, personal or business perspective, Oil India Limited has a fundamental responsibility to protect that information from unauthorized or accidental modification, loss or release. Furthermore, trustworthy and reliable information must be available to undertake and conduct OIL’s day-to-day business.

Specifically, information plays a vital role in core business processes and customer service, in contributing to operational and strategic business decisions, and in conforming to legal and statutory requirements. Accordingly, information must be protected to a level commensurate with its value to the organization.

3 OIL’s Approach to information security management

People, process, and technology are critical to OIL for the conduct of their activities. By developing, documenting, implementing and maintaining an Information Security Management System (ISMS) based on the ISO27001 standard, OIL will have greater confidence in its personnel and the information security framework, and offer better assurance to its customers.

An ISO27001 certification makes a public statement of capability, whilst permitting the organization to maintain the confidentiality, integrity and availability of its information. An ISO27001 certification also provides competitive advantage to OIL in the marketplace, as it puts OIL in the league of those infrastructure organizations that comply with a globally accepted and respected information security standard.
OIL has adopted a structured phased approach to information security risk management. The approach can be broadly classified into three distinct phases:

- Preparation of ISMS documentation (inclusive of all relevant records) in order to apply for certification;
- Implementation of the ISMS; and
- Certification process.

The various stages of the preparatory phase and the implementation of the ISMS are depicted below in Figure 1:

![Figure 1: ISO27001 Readiness and implementation approach](image)

4 Scope Definition Process

The scope of the Information Security Management System (ISMS) has been established based on discussions with IT Head and Concerned IT Personnel.
## 4.1 Business Understanding

Prior to finalizing the scope of the ISMS, discussions were held with the departments to obtain the following details:

- Information on the business activities;
- Key personnel; and
- IT infrastructure and processing environment that supports the business activities.

The information obtained during the first level of discussions with all the departments has been summarized below:

<table>
<thead>
<tr>
<th>Department</th>
<th>Inputs for scope definition</th>
</tr>
</thead>
</table>
| Information Technology | The department is responsible for the following main functions:  
• Managing and maintaining the IT infrastructure of OIL;  
• Maintaining applications that are being used by various business functions;  
• Provide the users with continuous technical and system support; and  
• IT Resource Planning and upgrading.  

**Key personnel:** Mr. Naba Jyoti Neog, Mr. Manoharan LR |
| Personnel           | The department is responsible for the following main functions:  
• Recruitment;  
• Performance Management System;  
• Compensation management; and  
• Exit process.  

**Key personnel:** Mr. Shyamal Baruah |
| Admin/Security       | The various functions of the Admin/ Security department are as follows:  
• Administration activities;  
• Physical Security Administration;  
• Maintenance of services and utilities; and  
• Logistics.  

**Key Personnel:** Mr. Golap CH. Medhi |
| Contracts            | The various functions of the Contracts department are as follows:  
• Preparation of contracts with Third Party Service Providers; and  
• Management of contractual issues.  

**Key personnel:** Mr. Atindra Roychoudhary |
5 Scope of ISMS

| Location | The facilities of OIL located at Duliajan, Assam and Noida in India are covered under the scope for this ISMS:  
|          | • OIL India Ltd.; 2nd Floor, R&D Building, Duliajan, Assam, India  
|          | • OIL India Ltd.; 3rd Floor, Plot No. 19, Sector 16A, Noida, Uttar Pradesh, India |
| Personnel | All employees of IT department of OIL located at the above facilities.  
|           | In addition, third party vendors working for IT department on the company premises are also covered under the scope of the ISMS. These include:  
|           | • Physical security staff;  
|           | • Housekeeping staff;  
|           | • External consultants in the Facilities department;  
|           | • Contract personnel; and  
|           | • Third party IT vendors. |
| Physical Assets | All Physical assets, which are in use by OIL for IT operations at the above, mentioned location.  
|               | Physical assets of OIL are like the following:  
|               | • Servers;  
|               | • Workstations;  
|               | • Backup devices;  
|               | • Network and communication equipment;  
|               | • CD’s and backup tapes;  
|               | • Communication links;  
|               | • Contracts;  
|               | • Master Service Agreements (MSA); and  
|               | • Printed/Blank documents. |
| Software | The following are the software assets of OIL:  
|           | Key application systems:  
|           | • SAP  
|           | • Biztalk  
|           | • E-Sampatti  
|           | • Land Information System  
|           | • Performance Management System  
|           | • Vendor Information System  
|           | • E&P Data Bank  
|           | Other software like:  
|           | • Server & Desktop Operating Systems;  
|           | • Network Management Systems; and  
|           | • Firewall, Intrusion Detection and other security related systems |
Information Assets

Information assets, both in electronic media and paper that are in use by OIL are considered in the scope of the ISMS.

The electronic information assets are like the following:

- Databases and data files for all projects;
- Project and process related artifacts;
- Accounting information;
- Payroll processing records;
- MIS reports;
- Budget information;
- Employee information database;
- Electronic documents maintained by each department; and
- Operational policies and procedures in electronic format.

The paper assets of OIL are like the following:

- Contractual documents;
- Master Service Agreements (MSA);
- Statutory records;
- Access log registers; and
- Policy/procedure documents in hard copies.

Services

Services supporting the computing infrastructure and work environment of OIL such as power supplies, air conditioning, UPS etc.

Scope limitation

The scope does not include

- Any other department of OIL
- Any other offices/facilities of OIL.
- Any OIL employee located at any other locations

Document Number: OIL-IS-ISMS-ISM-1.0

Version : 1.0

Oil India Limited
(A Government of India Enterprise)
## Document Details

<table>
<thead>
<tr>
<th>Title</th>
<th>ISMS Manual</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>1.0</td>
</tr>
<tr>
<td>Classification</td>
<td>Internal</td>
</tr>
<tr>
<td>Release Date</td>
<td>01.06.2013</td>
</tr>
<tr>
<td>Description</td>
<td>Document details the Information Security Management System for Oil India</td>
</tr>
<tr>
<td>Review Date</td>
<td>01.06.2013</td>
</tr>
<tr>
<td>Author</td>
<td>CISO</td>
</tr>
<tr>
<td>Reviewer/Custodian</td>
<td>CISO</td>
</tr>
<tr>
<td>Approved By</td>
<td>Information Security Council (ISC)</td>
</tr>
<tr>
<td>Owner</td>
<td>CISO</td>
</tr>
</tbody>
</table>

## Distribution List

<table>
<thead>
<tr>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Distribution Only</td>
</tr>
</tbody>
</table>

## Version History

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Version Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>01.06.2013</td>
</tr>
</tbody>
</table>
# Table of Contents

1. Introduction & Scope ........................................................................................................... 4  
2. Management Responsibility for ISMS .............................................................................. 10  
3. Review of the ISMS .......................................................................................................... 12  
   3.1. Review Input ............................................................................................................... 12  
   3.2. Review Output ........................................................................................................... 12  
   3.3. Internal ISMS Audits ............................................................................................... 13  
4. Management Review of the ISMS .................................................................................... 14  
5. ISMS Improvement Continual Improvement ................................................................... 14  
   5.1. Corrective action ....................................................................................................... 14  
   5.2. Preventive action ...................................................................................................... 14  
6. Gap analysis ..................................................................................................................... 15  
   6.1. Methodology ............................................................................................................. 15  
7. Risk assessment ................................................................................................................ 16  
   7.1. Objective .................................................................................................................. 16  
   7.2. Methodology ............................................................................................................ 16  
8. Risk treatment .................................................................................................................. 17  
   8.1. Objective .................................................................................................................. 17  
   8.2. Methodology ............................................................................................................ 17  
9. Statement of Applicability ............................................................................................... 17  
   9.1. Objective .................................................................................................................. 17  
   9.2. Methodology ............................................................................................................ 18  
10. Information Security Policy ............................................................................................. 19  
   10.1. Information Security Policy of Oil India ................................................................. 19  
   10.2. Principles ............................................................................................................... 20  
   10.3. Structure ............................................................................................................... 20  
      10.3.1. Oil India Information security policy ................................................................. 20  
      10.3.2. Oil India Information Security Policy Overview .............................................. 21  
      10.3.3. Information Security procedures ................................................................. 21  
      10.3.4. Information records ....................................................................................... 21  
2. Appendix: List of ISMS Documentation ........................................................................... 22
1. Introduction & Scope

This document details Oil India Private Ltd. Information Security Management System (ISMS). Information Security Management System (ISMS) is a part of the overall management system, based on the business risk approach, to establish, implement, operate, monitor, review, maintain and improve Information Security of an organization.

‘Information’ is an asset and consequently needs to be suitably protected. Information Security protects information assets from a wide range of threats in order to ensure business continuity, minimize business damage and maximize return on investments. Information Security is driven by the following control objectives:

- **Confidentiality** relates to the protection of sensitive information from unauthorized access.
- **Integrity** relates to the accuracy and completeness of information; as well as to the validity of information in accordance with business values and expectations.
- **Availability** relates to information being available when required by the business process. It also deals with safeguarding of necessary resources and associated capabilities.

The scope of the ISMS has been defined by the management of Oil India (Reference: OIL-IS-SD-Draft 0.1 (Oil India Scope Document)).

1.1. Information Security (IS) Policy

An IS policy has been deployed by the organization indicating the procedures to be followed.

(Refer: OIL-IS-POL-IS-Draft 0.1 (Information Security Policy))
1.2. Establishing Security Requirements

It is essential that Oil India identifies its security requirements. There are three primary sources for establishing these requirements:

- The first source is derived from Risk Assessment. In this approach, threats to assets are identified along with associated vulnerabilities; likelihood of threat materialization is evaluated and potential impact to business like theft of confidential information or unavailability of IT infrastructure is estimated.
- The second source is the legal, statutory, regulatory and contractual requirements that the organization, contractors, associates and service providers have to comply with like IT Amendment Act, 2008.
- The third source is the set of principles, objectives and requirements for information processing that an organization has developed to support its operations.

1.3. Process Approach to ISMS

Oil India has adopted the “Plan-Do-Check-Act” (PDCA) based approach for establishing, implementing, operating, monitoring, maintaining and improving the effectiveness of its ISMS. This process approach has enabled Oil India to emphasize the importance of:

- Understanding Oil India information security requirements and the need to establish an appropriate Information Security Policy and objectives for information security;
- Implementing and operating controls in the context of managing Oil India overall business risk;
- Monitoring and reviewing the performance and effectiveness of the ISMS; and
- Continual improvement based on objective measurement.
Application of PDCA model to ISMS process is briefly explained below:

1.3.1. Plan (Establishes the ISMS)

Oil India has adopted a structured phased approach to information security risk management. The approach can be broadly classified into three distinct phases:

- Preparation of ISMS documentation (inclusive of all relevant records) in order to apply for certification;
- Implementation of the ISMS; and
- Certification process.
The various stages of the preparatory phase and the implementation of the ISMS are depicted below in Figure 2:

**1.3.2. Do (Implements and Operates the ISMS)**

- Identification and evaluation of risk scores derived after risk assessment exercise is carried out for all assets.
- Risk management shall involve the selection of control objectives and identification of various controls for the treatment and management of the risk.
- Implementation of controls based on the Risk Assessment results.
- Risk Assessment plan is implemented to address the control objectives as identified in the Statement of Applicability
• Security Metrics are developed to measure the effectiveness of the implemented controls and provide benchmarks for control effectiveness.
• Implementation of all processes and procedures laid down in Information Security Policy Document and various other operating procedures.
• Creating awareness among users about Information security and their responsibilities towards Information security. Training, poster campaigns and other alternative methods will be employed to create awareness among users.

1.3.3. Check (Monitors and Reviews the ISMS)

ISMS Framework

Oil India Information Security Management System (ISMS) can be schematically represented as Figure 3.

![ISMS Framework Diagram]

Figure 3: Information Security Management Program

The ISMS core components are:
Awareness: The ISMS will include security awareness and training programs to ensure that all personnel understand how information security relates to their functions and will foster compliance with information security regulations.

- Monitoring procedures will be implemented.
- The roles and duties will be defined in Information security organization to ensure regular review of ISMS.
- Compliance with the Information Security Policy is also a core component of the ISMS.
- Periodic audits (quarterly) will be performed to review the performance of various controls and measures defined in ISMS.
- Management will conduct review of whole ISMS on annual basis. This kind of review will be based on various reports including Incident reports, internal audit reports and quarterly review reports.

1.3.4. Act (maintains and improves the ISMS)

- Oil India will implement the improvements identified by the audit committee/management to the ISMS and the same will be communicated to all interested parties.
- Follow up after management review of ISMS.
- Improvement of ISMS will also take account changing business environments as well as identification of new set of threats and its implications on business.

1.4. Documentation requirements

1.4.1. General

The following documents constitute the ISMS at Oil India:

- Oil India ISMS Scope Document;
- Oil India Information Security Policy;
- Oil India Risk Assessment Methodology;
Oil India Risk Assessment & Risk Treatment Report;

Oil India Statement of Applicability; and

Any other relevant supporting document and evidences.

1.4.2. Control of Documents

Reference: OIL-IS-POL-PCOD-Draft 0.1 (Oil India Procedure for Control of documents)

1.4.3. Control of Records

Reference: OIL-IS-POL-PCOR-Draft 0.1 (Oil India Procedure for Control of records)

2. Management Responsibility for ISMS

2.1 Periodic Review

The Chief Executive Officer (CEO) shall provide evidence of his commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS by:

- Establishing an information security policy;
- Establishing roles and responsibilities for information security and communicating to the organization along with the need to comply with information security policy and legal/regulatory requirements.
- Supporting ISC in communicating to Oil India the importance of meeting information security objectives and the need for continual improvement;
- Providing sufficient resources to develop, implement, operate and maintain the ISMS; and
- Carrying out reviews when necessary, and reacting appropriately to the results of these reviews.
2.2 Resource Management

2.2.1. Provision of resources

**Organization Structure**

**Information Security Council (ISC)**

- The ISC will serve as a body providing strategic direction to securing Oil India information/data, and will be reporting to the Chief Executive Officer.
- The ISC is supported by an Information Security Working Group (ISWG). Detailed roles and responsibilities of each of the above officials have been described in the Information Security Organization document.

2.3 Awareness and Training

ISMS do not guarantee security across Oil India and its subsidiaries even if all controls are in place, unless all employees discharge certain responsibilities and duties towards information security. The training will aim to explain each individual employee irrespective of level or grade about their role in maintaining information security and his/her responsibilities towards every information asset they handle. In order to ensure that the employees are adequately made aware of their DO’s and DON’T’s, suitable awareness trainings, visual aids, employee communication etc will be provided. Further it will be responsibility of every manager to ensure that the communication to his or her teams is complete and the ownership is clearly established. The time and commitment from senior management will also be devoted to furthering awareness across the Oil India.

Training on Information security and end user responsibilities shall be made a part of induction program for new employees.
3. Review of the ISMS

The ISC will review Oil India ISMS at-least 6 monthly to ensure its continuing suitability, adequacy and effectiveness to reflect the current business, technological and regulatory environments. This review will include assessing opportunities for improvement and the need for changes to the ISMS, including the security policy and security objectives. The results of the reviews will be clearly documented and records will be maintained.

3.1. Review Input

The input to ISMS review shall include information on:

- Results of ISMS audits and reviews;
- Feedback from interested parties;
- Techniques, products or procedures, which could be used in Oil India to improve the ISMS performance and effectiveness;
- Status of preventive and corrective actions;
- Vulnerabilities or threats not adequately addressed in the previous risk assessment;
- Follow-up actions from previous ISMS reviews;
- Changes that could affect the ISMS; and
- Recommendations for improvement.

3.2. Review Output

The output of the ISC review shall include any decisions and actions related to the following:

- Improvement of the effectiveness of the ISMS;
- Modification of procedures that effect information security, as necessary, to respond to internal or external events that may impact on the ISMS, including changes to:
  - Business requirements;
  - Security requirements;
3.3. Internal ISMS Audits

The Chief Internal Audit for Oil India shall conduct internal ISMS audits at planned intervals to determine the control objectives, controls, processes and procedures of its ISMS. The following audits will be carried out to determine the compliance with Oil India Information Security Policy and Procedures:

- Quarterly Compliance Audit;
- Half Yearly Self-Assessment; and
- Annual Audit.

The responsibilities and requirements for planning and conducting audits, and for reporting results and maintaining records will be defined in a documented procedure. Review of the ISMS documentation consists of two general categories: scheduled and unscheduled. Scheduled review is essentially time driven, while unscheduled review is event driven.

The respective business owner, responsible for the area being audited shall ensure that actions are taken without undue delay to eliminate detected non-conformities and their causes.
4. Management review of the ISMS

Management will be presented a quarterly report on the security metrics developed by Oil India. Also a yearly management review of ISMS will be conducted, which will suggest improvements to the ISMS including security metrics and information security policies and procedures.

Oil India will conduct risk assessments annually to identify and control risks owing to a changing business, technical and regulatory environment.

5. ISMS improvement Continual Improvement

The management shall ensure improvement of the ISMS on an ongoing basis by performing periodic reviews and, taking appropriate and timely decisions for effective implementation and maintenance of the ISMS.

5.1. Corrective action

The management will ensure appropriate corrective actions are taken to implement the required controls based on the review of the ISMS audit reports. The CISO will be responsible for presenting the internal ISMS audit reports, and explaining the resource requirements required to implement the controls to correct the gaps or non-conformities identified, to the management.

5.2. Preventive action

The management will ensure appropriate preventive actions are taken to implement the required controls based on the review of the ISMS audit reports. The CISO will be responsible for presenting the internal ISMS audit reports, and explaining the resource requirements required to implement the controls to prevent occurrence of perceived gaps.
or non-conformities to the management, keeping in view the changing business and security requirements of the business

6. Gap analysis

6.1. Methodology

Representatives from various departments are interviewed on the security controls implemented in the organization in compliance with ISO 270001 standard. The domains covered under this standard are as follows:

- Security policy;
- Organization of Information Security;
- Asset Management;
- Human Resources Security;
- Physical and Environmental security;
- Communications and Operations management;
- Access Control;
- Information Systems Acquisition Development;
- Information Security Incident Management
- Business continuity management; and
- Compliance.

The subsequent analysis primarily draws inputs from the review of the existence and adequacy of the documentation supporting Oil India’s information security framework.
The gap analysis assists Oil India in identifying the gaps and defining the target information security requirements, which it must adopt, in order to prepare for the ISO 270001 compliant ISMS.

(Reference: Oil India Gap Analysis Report)

7. Risk assessment

7.1. Objective
The objective of this risk assessment exercise is to identify areas of vulnerability and to initiate appropriate remediation. The risk assessment will result in identifying the assets and threats against those assets. These risks are prioritized based on the business impact and likelihood of risk occurring. Risk assessment helps ascertain the potential of the existing controls to mitigate these risks, so as to arrive at gaps that need to be addressed by the proposed Information Security Management System.

7.2. Methodology
Following steps are carried out for the Risk Assessment:

- Identification and Classification of the information assets;
- Deriving assets values by identifying the business impact of loss of confidentiality, integrity and availability of these assets;
- Grouping of assets that serve the business objective;
- Identification of the threats to these assets and the corresponding threat scores;
- Identification of the vulnerabilities in these assets that may be exploited by these threats and corresponding vulnerability scores;
- Mapping of threats and vulnerabilities to the assets; and
- Calculation of Overall Risk, existing control rating and existing residual risks.
8. Risk treatment

8.1. Objective

The Oil India management decides the acceptable level of risks after considering the existing residual risk or the proposed residual risk and the mitigation plan. In cases, where management decides to accept the existing residual risk i.e. authorization is not granted for implementation of controls, the reasons for the same are recorded. The risk treatment approach indicates the strategy adopted for each of the recognized threat.

8.2. Methodology

The risk treatment approach lists the threats and risk ratings arrived at in the Risk Assessment exercise. It decides on the risk treatment strategies to be adopted to treat each of the identified threats, based on the risk score. These strategies are:

- **Avoid the risk**: by deciding not to proceed with the activity or by choosing another way to achieve the same outcome;

- **Mitigate the risk**: by reducing either the likelihood of the risk occurring, the consequences of the risk or both;

- **Transfer the risk**: by shifting all or part of the risk to another party who is best able to control it; and

- **Accept the risk**: after accepting that it cannot be avoided, controlled or transferred.

9. Statement of Applicability

9.1. Objective

Once security requirements and risks have been identified and decisions for the treatment of risks have been made, an important step towards attaining ISO270001 preparedness is the identification and definition of information security control objectives, as applicable for
the specific business requirements of the organization to ensure risks are reduced to an acceptable level.

Part II of ISO 17799:2005 guidelines, Information technology — Security techniques — Code of practice for information security management, provides an extensive set of control objectives. However, all of these control objectives may not be applicable to Oil India business operations. Further, the control objectives outlined in ISO/IEC 17799:2005 Clauses 5 to 15 is not exhaustive and organizations may need to consider additional controls to be deployed to best suit its security needs.

Defining the Statement of Applicability (SoA) represents a significant step towards attaining ISO 270001 preparedness. The Statement of Applicability is a critique of the objectives and controls applicable to the needs of Oil India.

9.2. Methodology

The Statement of Applicability was developed, including the following:

- Control objectives/controls selected by Oil India along with appropriate justification of the selection; and

- Control objectives/controls (as stated in ISO/IEC 17799:2005 Clauses 5 to 15) not being considered by Oil India along with appropriate justification for their exclusion.

The SoA document is required to be made available to all managers, personnel and any third parties i.e. auditors, certifiers, etc., authorized to access it.
10. Information Security Policy

The purpose of this Information Security Policy is to provide the direction to the Information Security Council (ISC) and support for information security. The security policies have been established to cover information, data, business processes and communication networks used / operated by Oil India.

The objective is to measure the data security, by monitoring the Key Performance Indicators (KPI’s) for various departments as described in the Oil India’ Information Security Metric.

10.1. Information Security Policy of Oil India

Oil India’s Information Security Policy commits the Company to protect the security of its Information. It provides the same commitment to information entrusted to Oil India by its customers and business partners. We will deliver the above components in an integrated manner thorough an Information Security Management System that protects the Confidentiality, Integrity and Availability of Oil India’s information.

To meet this commitment we will:

• Maintain an effective Information Security Management System;
• Deploy most appropriate technology and infrastructure;
• Create and maintain a security conscious culture within the organization; and
• Continually monitor and improve the effectiveness of the Information Security Management System.

Responsibility for compliance with Oil India’s Security Policy and standards lies with the Chief Executive Officer, Centre of excellence (COE) Leaders and their staff.”
10.2. Principles

The Information Security Policies, Guidelines and Procedures at Oil India are consistent with the following principles:

- **Value driven**: Information security measures will be implemented in reasonable proportion to the risk and the business value of the information asset they intend to protect.

- **Accountability**: All users are accountable for their actions, as they relate to safeguarding of the information assets.

- **Least privilege**: Each user will be provided access to information assets based on ‘need-to-know’ and ‘need-to-do’ principles as required by their job profile.

- **Segregation of duties**: Separation of authority and responsibility will be carried out to ensure that an individual does not have sole control on all aspects of a particular information asset.

- **Integrity**: Security will be maintained at the level that it does not compromise the integrity of the trusted environment.

- **Scalable**: Security architecture will be maintained, so that the varying security needs of the organization can be accommodated.

10.3. Structure

The Oil India Information Security Policy consists of the following components:

10.3.1. Oil India Information security policy

This policy incorporates major controls outlined in the revised ISO17799, aligned to the ISO 27001 standard. The policy describes the technical and business processes that must be used to protect the confidentiality, integrity and availability of information.
While this document has broad coverage and applicability, it is not sufficient for every conceivable scenario. Therefore, it is not the sole information security policy that Oil India business should rely on.

There are many areas in this document that lay out the minimum security stance a business should take, or that present the principles that should be followed when making a business specific policy. In these areas, as in all other areas within this policy, controls and requirements are listed in addition to any business specific additions.

10.3.2. Oil India Information Security Policy Overview

This document provides a definition of Information Security, describes security responsibilities local to the business, and outlines the different components that make up the Oil India Information Security Policy.

10.3.3. Information Security procedures

Detailed Information Security Procedures have been developed to support the policies of Oil India.

Information security procedures provide the means for actualizing the information security policy. The security procedures lay down the step-by-step approach to implementing the information security policy. The information security procedures will involve defining, documenting, implementing, monitoring, and managing controls over information assets.

10.3.4. Information records

Information Records are established to support the Information Security Procedures
# 2 Appendix: List of ISMS Documentation

ISO 270001 core documentation
- ISO 270001 Scope Document;
- GAP Assessment Report;
- Information Security Organization;
- Risk Assessment & Risk Treatment Report;
- ISO 270001 Statement of Applicability;
- Oil India Information Security Management System Policy and procedures.

<table>
<thead>
<tr>
<th>ISO 270001 Domain / Sub-Domain</th>
<th>Document Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>4 Information security management system</strong></td>
<td></td>
</tr>
<tr>
<td>4.1 General requirements</td>
<td>ISMS Manual</td>
</tr>
<tr>
<td>4.2 Establishing and managing the ISMS</td>
<td>ISMS Manual</td>
</tr>
<tr>
<td>4.2.1 Establish the ISMS</td>
<td>ISMS Manual</td>
</tr>
<tr>
<td>4.2.2 Implement and operate the ISMS</td>
<td>Information Security Policy</td>
</tr>
<tr>
<td>4.2.3 Monitor and review the ISMS</td>
<td>Information Security Awareness Guidelines</td>
</tr>
<tr>
<td>4.2.4 Maintain and improve the ISMS</td>
<td>Internal Audit Procedure</td>
</tr>
<tr>
<td>4.3 Documentation requirements</td>
<td>ISMS Manual</td>
</tr>
<tr>
<td>4.3.1 General</td>
<td>ISMS Manual</td>
</tr>
<tr>
<td>4.3.2 Control of documents</td>
<td>Procedure for Control of Documents</td>
</tr>
<tr>
<td>4.3.3 Control of records</td>
<td>Procedure for Control of Records</td>
</tr>
<tr>
<td><strong>5 Management responsibility</strong></td>
<td></td>
</tr>
<tr>
<td>5.1 Management commitment</td>
<td>Information Security Policy</td>
</tr>
<tr>
<td>5.2 Resource management</td>
<td>ISMS Manual</td>
</tr>
<tr>
<td>Section</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>5.2.1</td>
<td>Provision of resources</td>
</tr>
<tr>
<td>5.2.2</td>
<td>Training, awareness and competence</td>
</tr>
<tr>
<td>6</td>
<td>Internal ISMS audits</td>
</tr>
<tr>
<td>8</td>
<td>ISMS improvement</td>
</tr>
</tbody>
</table>
Definitions Document

Document Number: OIL-IS-ISMS-DD-1.0

Version : 1.0

Oil India Limited
(A Government of India Enterprise)
# Document Details

<table>
<thead>
<tr>
<th>Title</th>
<th>Definitions Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>1.0</td>
</tr>
<tr>
<td>Classification</td>
<td>Internal</td>
</tr>
<tr>
<td>Release Date</td>
<td>01.06.2013</td>
</tr>
<tr>
<td>Description</td>
<td>Definitions of key terms used in various policy &amp; procedure documents</td>
</tr>
<tr>
<td>Review Date</td>
<td>01.06.2013</td>
</tr>
<tr>
<td>Author</td>
<td>CISO</td>
</tr>
<tr>
<td>Reviewer/Custodian</td>
<td>CISO</td>
</tr>
<tr>
<td>Approved By</td>
<td>Information Security Council (ISC)</td>
</tr>
<tr>
<td>Owner</td>
<td>CISO</td>
</tr>
</tbody>
</table>

## Distribution List

- Internal Distribution Only

## Version History

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Version Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>01.06.2013</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Information Asset</td>
<td>A component or product of an information system that can be defined, scoped, and managed for reuse.</td>
</tr>
<tr>
<td>Company</td>
<td>Oil India</td>
</tr>
<tr>
<td>Computer Systems</td>
<td>All computers whether server or client, all network equipment, infrastructure equipment, operating systems, messaging systems, software, output devices and storage mediums used to transmit, receive or view Company information</td>
</tr>
<tr>
<td>Information Technology (IT) Department</td>
<td>Department within Oil India responsible for Information Technology Assets</td>
</tr>
<tr>
<td>User</td>
<td>Employees and any other individuals who use Oil India Computer Systems</td>
</tr>
<tr>
<td>‘Must’, ‘Will’ and ‘Shall’</td>
<td>These terms mean that the detail is non-discretionary and must be implemented</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Ensuring that information is accessible only to those authorized to have access.</td>
</tr>
<tr>
<td>Integrity</td>
<td>Safeguarding the accuracy and completeness of information and processing methods.</td>
</tr>
<tr>
<td>Availability</td>
<td>Ensuring that authorized users have access to information and associated assets when required.</td>
</tr>
<tr>
<td>Policies</td>
<td>What needs to be done. Policy statements are produced by senior management to dictate how the organisation is going to achieve its objectives.</td>
</tr>
<tr>
<td>Standards</td>
<td>What we are using. Ensure that specific technologies, applications, parameters and procedures are carried out in a uniform way across the organisation.</td>
</tr>
<tr>
<td>Procedures</td>
<td>How we are doing it. Procedures show tasks required to be performed to adhere to the policies.</td>
</tr>
<tr>
<td>Guidelines</td>
<td>What helps us doing it. These are recommended actions and operational guides to users, IT staff, operations staff and others when a specific standard does not apply.</td>
</tr>
<tr>
<td>Production System</td>
<td>These are systems that are regularly used to process information critical to Oil India business. Such information systems have special security requirements.</td>
</tr>
<tr>
<td>Malicious software</td>
<td>Software deliberately designed to harm computing systems.</td>
</tr>
<tr>
<td>Sensitive information</td>
<td>Information that falls into the ‘Secret’ or ‘Confidential’ categories.</td>
</tr>
<tr>
<td>Service Level Agreements</td>
<td>Written agreement between a service provider and a customer that documents services and agreed service levels.</td>
</tr>
<tr>
<td>Administrator</td>
<td>A person employed to maintain and operate a computer system and/or</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>network</td>
<td>They may be members of an information technology department.</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Maintenance is the modification of a software product after delivery to correct faults, to improve performance or other attributes, or to adapt the product to a modified environment.</td>
</tr>
<tr>
<td>Local Area Network (LAN)</td>
<td>A computer network covering a small geographic area, like a home, office, or group of buildings.</td>
</tr>
<tr>
<td>Off-site Data</td>
<td>Data that is sent out of the main location as a part of disaster recovery plan/backup plan.</td>
</tr>
<tr>
<td>Software Library</td>
<td>A collection of software which help in the functioning of the organization.</td>
</tr>
<tr>
<td>Information</td>
<td>Knowledge of specific events or situations that has been gathered or received by communication; intelligence or news.</td>
</tr>
<tr>
<td>User Account</td>
<td>An established relationship between a user and a computer, network or information service.</td>
</tr>
<tr>
<td>Operating System</td>
<td>An operating system (commonly abbreviated OS and O/S) is the software component of a computer system that is responsible for the management and coordination of activities and the sharing of the resources of the computer.</td>
</tr>
<tr>
<td>Database Management System (DBMS)</td>
<td>Software that manages, manipulates and retrieves data in a database.</td>
</tr>
<tr>
<td>Application</td>
<td>It is a subclass of computer software that employs the capabilities of a computer directly and thoroughly to a task that the user wishes to perform.</td>
</tr>
<tr>
<td>Network Equipment</td>
<td>Equipment facilitating the use of a network.</td>
</tr>
<tr>
<td>Authentication</td>
<td>The act of establishing or confirming the presence of a user.</td>
</tr>
<tr>
<td>IP Source Routing</td>
<td>It allows a sender of a packet to specify the route the packet takes through the network.</td>
</tr>
<tr>
<td>Secure Socket Layer</td>
<td>Provide secure communications on the Internet for such things as web browsing, e-mail, Internet faxing, instant messaging and other data transfers.</td>
</tr>
<tr>
<td>Firewall</td>
<td>A device or set of devices configured to permit, deny, encrypt, or proxy all computer traffic between different security domains based upon a set of rules and other criteria.</td>
</tr>
<tr>
<td>Broadcast Address</td>
<td>An IP address that allows information to be sent to all machines on a given subnet rather than a specific machine.</td>
</tr>
<tr>
<td>Operating System Hardening</td>
<td>It is the first step towards safeguarding systems from intrusion; it involves The removal of all non essential tools, utilities and other systems administration options, any of which could be used to ease a hacker's path to your systems.</td>
</tr>
<tr>
<td>Network Protocol</td>
<td>It’s a convention or standard that controls or enables the connection,</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Network Interface</td>
<td>The point of interconnection between a user terminal and a private or public network, or between one network and another network.</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol (SNMP) is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. It consists of a set of standards for network management.</td>
</tr>
<tr>
<td>Firewall Appliance</td>
<td>A dedicated hardware and software system whose sole purpose is to function as the implementer of the defined access control policy.</td>
</tr>
<tr>
<td>Super User</td>
<td>A special user account used for system administration.</td>
</tr>
<tr>
<td>Screen Saver</td>
<td>A screensaver is a type of computer program initially designed to prevent “Phosphor burn-in” on CRT and plasma computer monitors by blanking the screen or filling it with moving images or patterns when the computer is not in use.</td>
</tr>
<tr>
<td>Password Protect</td>
<td>The use of a sequence of characters that must be entered in order to gain access to electronically locked or protected computer or security systems, files, etc.</td>
</tr>
<tr>
<td>Vulnerability</td>
<td>A weakness in a system which allows an attacker to violate the integrity of that system. Vulnerabilities may result from weak passwords, software bugs, a computer virus or other malware.</td>
</tr>
<tr>
<td>Information Owner</td>
<td>A designated personnel identified as custodian of the information assets at the Company responsible for ensuring that information and assets associated with information processing facilities are appropriately classified and defining and periodically reviewing access restrictions and classifications, taking into account applicable access control policies.</td>
</tr>
<tr>
<td>Change Approver</td>
<td>Designated personnel identified for approval of changes and to be informed in case of any escalations.</td>
</tr>
<tr>
<td>Change Originator/Requester</td>
<td>Personnel who have the authority to raise change requests and provide all the required information for implementing the change.</td>
</tr>
<tr>
<td>Incident</td>
<td>An unplanned interruption to or reduction in the quality of IT Service.</td>
</tr>
</tbody>
</table>

Document Number: Oil-IS-ISMS-ISO-1.0

Version : 1.0
## Document Details

<table>
<thead>
<tr>
<th></th>
<th>Signatures with Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Procedure for Control of Corrective and Preventive Actions</td>
</tr>
<tr>
<td>Version</td>
<td>1.0</td>
</tr>
<tr>
<td>Classification</td>
<td>Internal</td>
</tr>
<tr>
<td>Release Date</td>
<td>01.06.2013</td>
</tr>
<tr>
<td>Description</td>
<td>Details of the Information Security Organization structure and the roles and responsibilities of the organization</td>
</tr>
<tr>
<td>Review Date</td>
<td>01.06.2013</td>
</tr>
<tr>
<td>Author</td>
<td>CISO</td>
</tr>
<tr>
<td>Reviewer/Custodian</td>
<td>CISO</td>
</tr>
<tr>
<td>Approved By</td>
<td>Information Security Council (ISC)</td>
</tr>
<tr>
<td>Owner</td>
<td>CISO</td>
</tr>
</tbody>
</table>

## Distribution List

<table>
<thead>
<tr>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Distribution Only</td>
</tr>
</tbody>
</table>

## Version History

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Version Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>01.06.2013</td>
</tr>
</tbody>
</table>
# Table of Contents

1. Introduction .................................................................................................................. 4
2. Information Security Council (ISC) ............................................................................... 4
2.1 Roles and Responsibilities ............................................................................................ 5
  2.1.1 Information Security Steering Group (ISSG) ......................................................... 5
  2.1.2 Chief Information Security Officer (CISO) .......................................................... 6
  2.1.3 Information Security Working Group (ISWG) ....................................................... 8
  2.1.3 Information Security Audit team (ISA) ................................................................. 10
1. Introduction

Oil India Limited (hereafter referred as OIL), a premier National Oil Company, is engaged in the business of Exploration, Production and Transportation of Crude Oil and Natural Gas from defined concessional areas in Upper Assam and Arunachal Pradesh and parts of eastern, northern and western India. Oil India Private Limited was incorporated on 18th February 1959 as a partnership venture between the Government of India and the BOC for the management of Nahorkatiya and Moran discoveries. On 14 October 1981 Oil India became wholly owned Government of India enterprise. OIL operates in India from its offices locations in Upper Assam, Arunachal Pradesh and parts of eastern, northern and western India.

2 Information Security Council (ISC)

![Information Security Organization Structure](image)

**Figure 1: Information Security Organization Structure**
2.1 Roles and Responsibilities

2.1.1 Information Security Steering Group (ISSG)

The ISC will undertake the following:

- Decide and approve the scope of Information Security Management System (ISMS).
- Appoint the Chief Information Security Officer (CISO) and provide adequate resources to support and coordinate the implementation of security.
- Provide information security directives across the organization.
- Formulate, monitor, review and approve the organization’s Information Security Policies and overall responsibilities.
- Provide direction and support for the implementation of ISMS and constantly strive to improve the ISMS.
- Obtain clear understanding and monitor significant changes in the exposure of information assets to various threats being faced by the organization and support new initiatives to improve ISMS.
- Review and monitor major incident reports provided by the CISO, together with the results of any investigation carried out.
- Promote information security education, training and awareness throughout Oil India.
- Ensure that all users are aware of their security roles and responsibilities.
- Review all the policies at least on an annual basis or as deemed necessary. The CISO takes responsibility of ensuring that the policy is regularly reviewed and any recommendations to the same shall be promptly presented to the ISC.
- Review internal audit report on ISMS and follow-up on the status of correction actions taken.
**OIL-IS-ISMS- ISO-1.1 (Information Security Organization)**

- Review the Executive Summary of audit reports annually.
- Identify and address legal and regulatory requirements and contractual security obligations of the organization.
- Identify, classify and periodically review the criticality and confidentiality requirements of all types of information resources.

The Information Security Council will meet at least once a year to assess the security requirements of Oil India or as required by any significant change in the business operating environment. Members of ISC may depute their representative for mandatory review meetings.

### 2.1.1. Chief Information Security Officer (CISO)

The Chief Information Security Officer (CISO) will be a part of the Information Security Working Group (ISWG) with reporting to Information Security Council (ISC) that is the governing body for the Information Security Organization. She/he will have the following responsibilities:

- Manage the overall Information Security program at Oil India.
- Ensure that the Information Systems Security Policies, procedures and recommended practices for use throughout Oil India are updated in a timely manner to represent all current modifications.
- Ensuring that the information security policy is reviewed once a year (at least) for any changes in the IT or business environment.
- Identify emerging trends in the industry vertical (within which the organization is currently poised), in relation to safety and security measures.
- Point of contact to the business managers and IT Unit on information security implementation and non-compliances and to ensure that an effective process for implementing and maintaining the security controls is in place.
OIL-IS-ISMS- ISO-1.1 (Information Security Organization)

- Serve as a supervisor for all the security specialists and enforce information security policies and recommended practices.

- Ensure that the security requirements for new information processing facilities have been identified and approved. Ensure that the requisite policies and standards are developed.

- Ensure that an appropriate technical architecture is defined for the security of IT infrastructure and monitor compliance with the same.

- Allocate roles and responsibilities for information security to individuals within the IT team and ensure that they dispose their responsibilities.

- Arrange required resources and skills for conducting periodic information security reviews.

- Encourage the participation of the managers, auditors, legal department and the staff members from various disciplines, who can contribute to compliance with information security practices.

- Define and communicate to the management, the key threats to the information assets at various point of time.

- Ensure that appropriate security controls are defined for all applications in consultation with the application owner (Note: Certain client security requirements may supersede some of Oil India information security requirements).

- Maintain and review all critical incidents that have occurred and the corresponding resolution timeframe and apprise the ISC of the same.

- Involve in-house security specialists or external specialists where required for addressing specific information security requirements.

- Plan and organize internal audits of information security at periodic intervals either by internal auditors or external agencies.
**OIL-IS-ISMS- ISO-1.1 (Information Security Organization)**

- Coordinate any Incident Response procedures undertaken in response to potential security breaches.
- Coordinate or assist in the investigation of security threats or other attacks on the information assets.
- Report security incidents and violations to the ISC.
- Ensure that adequate security training is provided to various end users and security awareness programs are conducted regularly.
- Review and approve the prioritization plan for implementation of patches and fixes for vulnerabilities that are identified from time to time.

### 2.1.2. Information Security Working Group (ISWG)

The Information Security Working Group (ISWG) is entrusted with the responsibility of managing security related operations on a day-to-day basis and co-ordinating with the IT team for implementation/maintenance of the ISMS. The ISWG will meet on quarterly basis for the same. They will have the following responsibilities:

- Develop and maintain the Information Systems Security Policies, procedures and Standards for use throughout Oil India.
- Ensure that all critical operations are carried out in accordance with the security guidelines.
- Work with the CISO to ensure that an effective process for implementing and maintaining the security controls is in place.
- Remain current/up-to-date on the threats against the information assets (attending information security meetings, reading trade publications and participation in work groups are some of the ways to stay current/up-to-date with the developments in the field of information systems security).
- Understand the current information processing technologies and information security practices by receiving internal education, attending information security seminars and through on-the-job training.
**OIL-IS-MS- ISO-1.1 (Information Security Organization)**

- Understand the business processes of the organization, so as to provide appropriate security protection.

- Review, audit and examine reports dealing with the information security issues and ensure that they are presented to the CISO at pre-determined intervals.

- The ISWG should be involved in the formulation of the management’s response to the audit findings and follow-up to ensure that the security controls and procedures, as required, are implemented within the stipulated time frame.

- Define and communicate to the CISO, the key threats to the information assets.

- Assume responsibility or assist in the preparation and distribution of an appropriate warning system of potentially serious and imminent threats to Oil India’s information assets e.g. outbreak of computer virus etc..

- Assist in responding to the security issues relating to the customers including the letters of assurance and suitable replies to the questions on information systems security, as and when raised by the customers.

- Ensuring that the systems and network are secure and that any breach is quickly identified analyzed and fixed.

- Coordinate any Incident Response procedures undertaken in response to (current /potential) security breaches.

- Coordinate or assist in the investigation of security threats or other attacks on the information assets.

- Assist in the recovery of information and information assets from such attacks.

- Prepare, maintain and test contingency plans or disaster recovery plans.

- Conduct network and system reviews from time to time to check for policy compliance and loopholes, (if any), in the infrastructure. This could be done using approved automated tools to save time and provide user friendly reporting.

- Report security incidents and violations to the CISO.
**OIL-IS-ISMS- ISO-1.1 (Information Security Organization)**

- Ensure that adequate security training is provided to various end users and security awareness programmes are conducted regularly.

- Ensure that basic security training is provided to IT team from time to time. This responsibility also covers that any new IT staff members be given a security briefing at the time of joining.

- Preparation of prioritization plan for implementation of patches and fixes for vulnerabilities that are identified from time to time.

- Provide a monthly update to the CISO regarding the status of information security initiatives. It should include:
  - Any observed non-compliances/major incidents reported/managed
  - Corrective and Preventive Actions require

**2.1.3. Information Security Audit team (ISA)**

The Internal Audit team (IA) is entrusted with the responsibility of ensuring compliance with ISMS framework in all aspects. The IA team will meet on biannually basis for the same. They will have the following responsibilities:

- Conduct internal audits to assess conformance to the standard, organization’s policies, effectiveness of implementation and maintenance.

- Define and document procedures including responsibilities and requirements for planning and conducting audits, and for reporting results and maintaining records.

- Evaluates organization’s compliance with ISMS framework in all aspects.

- Detects any shortcomings in the implementation of ISMS framework within the organization

- To ensure deployment of robust information security framework.

- To recommend the necessary corrective and preventive actions.

- To ensure continuous improvement of information security controls.
Information Security Awareness Guidelines

Document Number: OIL-IS-GUD-ISA-1.0

Version: 1.0
This document provides guidelines for setting up information security awareness across the organization.

<table>
<thead>
<tr>
<th>Version History</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Version Number</strong></td>
</tr>
<tr>
<td>Draft 0.1</td>
</tr>
<tr>
<td>1.0</td>
</tr>
</tbody>
</table>
# OIL-IS-GUD-ISA-1.0 (Information Security Awareness Guideline)

## Table of Content

1. **Purpose** ........................................................................................................................................... 4
2. **Guidelines** ........................................................................................................................................ 4
   2.1 Information Security Awareness Program (ISAP) .......................................................................... 4
      2.1.1 Goals and Principles .................................................................................................................. 4
      2.1.2 Assumptions ................................................................................................................................ 5
   2.2 Information Security Awareness Campaign (ISAC) ....................................................................... 5
      2.2.1 Programs within the ISAC ......................................................................................................... 5
      2.2.2 Project Development .................................................................................................................. 6
   2.3 Information Security Training Program (ISTP) .............................................................................. 6
      2.3.1 Training Channels ...................................................................................................................... 6
      2.3.2 ISTP Phases ............................................................................................................................... 7
      2.3.3 ISTP Topics ............................................................................................................................... 8
1. Purpose

The purpose of this document is to provide guidelines for setting up information security awareness program at the Company.

This guideline for Information Security Awareness Program (ISAP) supports the high level policy statements defined in the Company’s Information Security Policy. The purpose of the ISAP is to assist all users in becoming more knowledgeable and conscious of their responsibilities in securely generating, using, and maintaining the information assets of the Company.

It is the responsibility of the Information Security Manager (ISM) to initiate steps to make all employees aware of those practices, which promote secure and sensible information management. It will provide all employees with the basic knowledge needed to handle data in a secure manner.

The ISAP will consist of the following initiatives:

- Information Security Awareness Campaign (ISAC); and
- Information Security Training Program (ISTP)

Intended Audience

All employees and third party employees of the Company will participate in the awareness campaigns and training programs organized by the Information Security Council (ISC).

2. Guidelines

2.1. Information Security Awareness Program (ISAP)

2.1.1. Goals and Principles

The goal of this program is to “change behavior by changing attitudes”. This is a program of education and awareness. The program will develop the user’s knowledge, skills and abilities so that the users can perform their jobs more securely. The ultimate goal is to ensure that all Company’s employees appropriately handle and protect all Information Assets.

In many cases this means changing the information handling behavior of the employees. The ISAP aims to do this through a systematic program of awareness enhancement and education in
secure computing and information handling practice(s). This program is designed to make users aware of their own attitudes about such practices, as well as to communicate the most appropriate attitudes.

2.1.2. Assumptions

A key consideration for the creation and planning of an ISAP is the time/resources we will commit to such a program. In formulating this program the following assumptions are made with regards to the availability of the Company’s employees and resources needed to execute the program:

- All new employees of the Company will be made available for at least one hour to participate in ISTP;
- Resources will be made available as required for the development of Company approved information security training material and training programs;
- The Company’s executive leadership will review and support ISAP.

2.2. Information Security Awareness Campaign (ISAC)

In support of the Company’s ISAP, an ISAC will be organized and executed through the office of the Information Security Manager. The content and scope of these programs will be developed by the IT Department and then reviewed and approved by the Information Security Manager.

2.2.1. Programs within the ISAC

Some of the programs that may be implemented by the ISC for instilling security awareness are:

- Security Awareness Week – A week designated as “Security Awareness Week” may be announced and observed with every security awareness project possible. Such a week will act as a focus point to initiate or enhance other projects and to raise employee awareness regarding the importance of information security.
- Electronic Mail – Bulletins addressing information security topics may be developed and may include descriptions of security incidents, possible impact of security breaches, and how an effective security posture can act as an enabler for business operations.
- Posters – Posters may be created with Information Security themes and posted at common meeting locations to heighten user awareness of security issues.
• Screensavers – The security awareness project team could develop screensavers to provide and improve information security awareness.

2.2.2. Project Development

The security awareness program team will staff each of these programs as well as any others that are recommended by the ISM or the Company’s management. Each project may be presented to the authorities for all required approvals. It is assumed that resources may need to be designated to facilitate the implementation and to offset the cost required for any of the projects listed above.

2.3. Information Security Training Program (ISTP)

In addition to the ISAC, the Company needs more formalized and structured training for users to ensure that they have adequate knowledge necessary to securely perform their duties.

In order to provide an effective and efficient ISAP, the Company may institute an ISTP in components targeted at end users.

2.3.1. Training Channels

The ISTP may use all possible channels for providing training in order to fully utilize modern training technologies. The types of channels that may be used include:

• Class-room training sessions;
• Monthly question and answer sessions; and
• Self-paced computer based training.

The training channels may also be integrated with the organizations’ regular activities like the following:

• Employee induction programs;
• Town Halls; and

• “Security Moments” in meetings.
2.3.2. ISTP Phases

The information security training requirements may be identified by the ISC. A training program development project may be created to develop the required training resources.

In those cases where it will meet training objectives in a more efficient manner, the training program development team may opt to obtain commercial off-the-shelf training material.

**Analysis**

An assessment of training needs may be conducted to determine the training objective and the level of the target audience. The assessment will also determine whether training is, in fact, the appropriate solution. Training will solve problems that relate to knowledge and skill deficiencies on the part of the users. Thus, training need is clearly indicated when employees are new or when new technologies or procedures are introduced to an existing work force. Assessment of training needs determines who must be trained, what instructional methods must be used to train, and what delivery options (or channels) exist for training.

**Design**

Once it has been determined that training is actually needed, the next step is to systematically define the content of the training program. This facilitates the creation of an appropriate content for the ISTP.

**Development**

The development phase involves the preparation of the training material to be used by the trainer/ trainee.

**Instruction**

Once the security training has been fully developed, small-scale training sessions may be arranged to validate the course material (see Evaluation Phase below). Once the course material has been validated, the Information Security Training team will arrange for the following:

- Support within the Company;
- Instructors (if necessary);
- Sufficient available time for the course participants;
OIL-IS-GUD-ISA-1.0 (Information Security Awareness Guideline)

- Space for the instruction;
- Course materials in sufficient quantity for all instructors and participants; and
- Any required audio and/or video support for the instruction.

**Evaluation & Maintenance**

Course material inevitably contains sections that can be improved upon. A well-organized security training evaluation program is necessary to ensure that training is valid and correctly performed. The ISTP team may ensure that resources are available to evaluate the performance of the instructors as well as to solicit feedback from the learners regarding the course content and administration.

Based upon the feedback from learners, the ISTP team must ensure that security training course material is updated in a timely manner and that any deficiencies in instructor performance are remedied.

The training material and awareness campaigns need to be revised and evaluated based on the following changes:

- Need based changes;
- Change in business processes or operations; and
- Changes to the Information Security policy.

**2.3.3. ISTP Topics**

Topics that may be considered for inclusion in ISTP include:

- Acceptable policies/guidelines for information technology resources;
- Electronic mail policies/guidelines;
- Internet security issues; and
- Security incident reporting and handling requirements
## Document DETAILS

<table>
<thead>
<tr>
<th>Title</th>
<th>Segregation of Duties Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>1.0</td>
</tr>
<tr>
<td>Classification</td>
<td>Internal</td>
</tr>
<tr>
<td>Release Date</td>
<td>01.06.2013</td>
</tr>
<tr>
<td>Description</td>
<td>Segregation of Duties Guidelines</td>
</tr>
<tr>
<td>Review Date</td>
<td>01.06.2013</td>
</tr>
<tr>
<td>Author</td>
<td>CISO</td>
</tr>
<tr>
<td>Reviewer/Custodian</td>
<td>CISO</td>
</tr>
<tr>
<td>Approved By</td>
<td>Information Security Council (ISC)</td>
</tr>
<tr>
<td>Owner</td>
<td>CISO</td>
</tr>
</tbody>
</table>

## Distribution List

<table>
<thead>
<tr>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Distribution Only</td>
</tr>
</tbody>
</table>

## Version History

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Version Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>01.06.2013</td>
</tr>
</tbody>
</table>
# Table of Contents

1. Introduction ................................................................................................................ 4  
2. Purpose of Segregation of Duties ............................................................................. 4  
3. Principle of Segregation of Duties ........................................................................... 4  
4. Identification of Segregation of Duties Issues .......................................................... 5  
5. Remediation of Segregation of Duties Issues ............................................................ 6
1. Introduction

Segregation of Duties is the separation of incompatible duties that could allow one person to commit and conceal fraud that may result in financial loss or misstatement to the company. Segregation of duties may be within an application or within the infrastructure. It represents a key internal control that ensures no single person has too much influence over any business transaction or operation. It serves to prevent unintentional errors or fraud and ensure timely detection of errors that may occur. Further, it provides a method of improving organizational, business process and IT control alignment. Segregation of duties has always been an important component of a properly functioning internal control environment.

2. Purpose of Segregation of Duties

Adequate segregation of duties reduces the likelihood that errors (intentional or unintentional) will remain undetected by providing for separate processing by different individuals at various stages of a transaction and for independent reviews of the work performed. The segregation of duties provides four primary benefits: 1) the risk of a deliberate fraud is mitigated as the collusion of two or more persons would be required in order to circumvent controls; 2) the risk of legitimate errors is mitigated as the likelihood of detection is increased; 3) the cost of corrective actions is mitigated as errors are generally detected relatively earlier in their lifecycle; and 4) the organization’s reputation for integrity and quality is enhanced through a system of checks and balances.

Segregation of duties is a basic, key internal control and one of the most difficult to accomplish. In essence, there is greater assurance that internal control responsibilities will be fully deployed when there is increased dispersion of such responsibilities among multiple individuals and work groups.

3. Principle of Segregation of Duties
The key principle of segregation of duties is that an individual or small group of individuals should not be in a position to control all aspects of a transaction or business process. Basically, the general duties to be segregated are: planning/initiation, authorization, custody of assets, and recording or reporting of transactions. In addition, control tasks such as review, audit, and reconcile should not be performed by the same individual responsible for recording or reporting the transaction.

The principle of segregation of duties generally helps define the constructs that will govern the definition of processes, controls and reporting structures of organizational units.

The principle of segregation of duties in an information system environment is also critical as it ensures the separation of different functions such as transaction entry, on-line approval of the transactions, master file initiation, master file maintenance, user access rights, and the review of transactions. In the context of application level controls, this means that one individual should not have access rights that permit them to enter, approve and review transactions. Therefore, assigning different security profiles to various individuals would support the principle of segregation of duties.

4. Identification of Segregation of Duties Issues

- Each functional business area shall be responsible for developing and implementing a schedule for assessing its area for potential or actual segregation of duties on a recurring basis.

- Each functional business area shall formally evaluate its area for the existence of potential or actual segregation of duties issues on a periodic basis.

- Organizational segregation of duties issues shall be considered during the periodic evaluations. The positioning of the business area in company, its relationships with other functional business areas, and the nature of its responsibilities shall be considered.

- Functional segregation of duties issues shall be considered during the periodic evaluations. The assigned job functions of personnel in the business area shall be considered from a standpoint of incompatible duties.
OIL-IS-GUD-SOD-1.0 (Segregation of Duties Guidelines)

- Technological segregation of duties issues shall be considered during the periodic evaluations. The assigned system and application security of personnel shall be considered from a standpoint of access within systems to perform incompatible functions.

5. Remediation of Segregation of Duties Issues

- Each functional business area shall document the segregation of duties issues identified during the formal periodic evaluations.

- The nature of the issue and the involved parties/systems shall be included in the documentation of the segregation of duties issues.

- Business area management shall review the documentation and determine remediation options for each issue.

- Remediation options may include a combination of corrective or mitigating measures.

- Business area management shall document the selected remediation method, along with the effective date of the remediation.

- Senior management and Internal Audit shall be provided copies of all documentation relating to segregation of duties analysis and remediation.
**Document Details**

<table>
<thead>
<tr>
<th></th>
<th>Signatures with Date</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Title</strong></td>
<td>Asset Management Policy</td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>Version 1.0</td>
</tr>
<tr>
<td><strong>Classification</strong></td>
<td>Internal</td>
</tr>
<tr>
<td><strong>Release Date</strong></td>
<td>01.06.2013</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Management of Information assets at Oil India Limited</td>
</tr>
<tr>
<td><strong>Review Date</strong></td>
<td>01.06.2013</td>
</tr>
<tr>
<td><strong>Author</strong></td>
<td>CISO</td>
</tr>
<tr>
<td><strong>Reviewer/ Custodian</strong></td>
<td>CISO</td>
</tr>
<tr>
<td><strong>Approved By</strong></td>
<td>Information Security Council (ISC)</td>
</tr>
<tr>
<td><strong>Owner</strong></td>
<td>CISO</td>
</tr>
</tbody>
</table>

**Distribution List**

<table>
<thead>
<tr>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Distribution Only</td>
</tr>
</tbody>
</table>

**Version History**

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Version Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 1.0</td>
<td>01.06.2013</td>
</tr>
</tbody>
</table>
# Table of Contents

1. Purpose .................................................................................................................................4
2. Policy ....................................................................................................................................4
   2.1 Application .........................................................................................................................4
   2.2 Software Asset Management .............................................................................................4
   2.3 Hardware Asset Management .............................................................................................5
      2.3.1 Information Asset Management ........................................................................5
      2.3.2 Process for Equipment Maintenance ........................................................................7
      2.3.3 Process for Equipment Repairs ..............................................................................7
         2.3.3.1 Identification Process ......................................................................................7
         2.3.3.2 Resolution Process ...........................................................................................8
      2.3.4 Media Management ....................................................................................................8
      2.3.5 Process for Removal of Equipment / Property .........................................................9
      2.3.6 Process for Returnable Equipments ..........................................................................9
      2.3.7 Disposal or Transfer of Equipments ..........................................................................9
3. Non Compliance ...................................................................................................................10
1 Purpose

This Policy supports the high level policy statements defined in Information Security Policy. Asset Management encompasses planning, demand, acquisitions, usage, maintenance, and disposal of information assets in order to achieve efficient and effective service delivery. The purpose of this policy is to govern the management of IT assets used and/or owned by Oil India to ensure that they are managed, controlled, safeguarded and used in an efficient and effective manner.

2 Policy

2.1 Application

This policy document applies to all organizational information assets being used at Oil India, which includes, but not limited to, the following:

- Software Assets;
- Workstations;
- Servers which includes Email server, gateway/firewall server, backup server and ftp server etc;
- Other IT Network Infrastructure which includes routers, switches etc; and
- Hardcopy and softcopy documents containing organization’s information.

2.2 Software Asset Management

Software Asset management includes maintaining software license compliance; tracking the inventory and usage of software assets; and maintaining control over the deployment, and use of software assets.

- Procurement details, such as number of licenses granted, expiry date of licenses, etc., of software purchased will be recorded in a centralized repository by the IT Department.
• Data in software inventory will be synchronized with software purchase data e.g. date of purchase, expiry date of the license and number of licenses etc. Original physical copy of the license received from the vendor, if any, on purchase shall be filed appropriately and stored securely.

• Software usage and deployment will be tracked and reconciled against purchase data on a quarterly basis. Any discrepancies, if observed, will be reported to the asset owner and the IT Manager.

• In case software license agreements are found to be violated, the IT Head will be informed by IT Manager and immediate corrective actions will be taken as applicable.

• Software purchases and related data will be tracked and regularly monitored. IT Manager, along with respective business owner of the applications, will be responsible for conducting annual reviews on this data to determine, but not limited to, the following:
  − If more licenses have been purchased than required;
  − If multiple software have been deployed with overlapping functionality and to serve the same purpose; and
  − If new software or more number of licenses need to be procured to meet future business requirements.

• IT Department will conduct annual review of servers and desktops to determine if any unauthorized and unlicensed software are installed and ensure:
  − Required service packs or security patches are installed; and
  − Minimum requirements for upcoming OS or software migrations are met.

2.3 Hardware Asset Management

2.3.1 Information Asset Management

• An asset class must be defined for all types of information assets e.g. Hardware, Software, IT Infrastructure etc. An inventory of assets will be maintained by the Asset Class owners for each class of assets defined. The asset owners will be identified for all the assets and they
will be responsible for successful execution and completion of the following activities which includes:

- Maintaining the asset;
- Safeguarding the asset and asset documentation;
- Classify the assets as per the Data Classification Policy;
- Renewing any contracts /agreements /licenses associated with the asset at required intervals;
- Conducting periodic audits to ensure compliance to the organization’s policies and procedures;
- Safeguarding all media (floppy disks, CDs or other storage media used to install the software / store data) associated with the asset; and
- Maintaining all original manuals and reference documentation (if any).

The asset owner will identify the custodian for the asset who will be responsible for the following activities:

- Follow the instructions of Owners, operate systems on behalf of Owners to serve users authorized by Owners;
- Define the technical options, such as information criticality categories, and permit Owners to select the appropriate option for their information;
- Define information systems architectures and provide technical consulting assistance to Owners so that information systems can be built and run to optimal meet business objectives;
- If requested, provide reports to Owners about information system operations and information security issues; and
- Safeguard the information in their possession, including implementing access control systems to prevent inappropriate disclosure, and developing, documenting, and testing information systems contingency plans.
2.3.2 Process for Equipment Maintenance

- Periodic equipment maintenance will be handled by the IT Department to ensure that all equipments are maintained as per the manufacturer’s specifications.

- At the end of warranty period, an Annual Maintenance Contract (AMC) will be drawn with the third party vendor for all equipments in Oil India. A scheduled inspection and maintenance chart with equipment details, frequency, responsibility etc. will be maintained and updated on semi-annual basis.

- Following equipment maintenance details will be included in the Asset list maintained by the IT department:
  - Equipment details including serial number and quantity;
  - Start and end Date of AMC contract;
  - Warranty details; and
  - Third party vendor contact details.

- In the event of a failure of service from the vendor, the escalation process as specified in the AMC will be followed.

2.3.3 Process for Equipment Repairs

2.3.3.1 Identification Process

- Any equipment repair observed by employees on workstations, laptops and servers will be reported to the IT Department.

- The IT Department will be responsible for recording the problem, prioritizing the requests and reporting the same based on the severity level.

- Any equipment repair observed by employees on building infrastructure related equipments will be reported to the Administration.
2.3.3.2 Resolution Process

- The third party vendor will be consulted for all equipment repairs under warranty and the IT Manager will ensure that the warranty of the equipment is not compromised.
- In the event of a repair wherein the equipment needs to be sent off-premises, appropriate authorization will be taken from the IT Manager.
- In case a third party, such as a document management company or a courier service is used for transport of electronic media, it will be adequately protected. Electronic / printed media in transit will be properly packed to prevent damage.
- On return of equipment, the IT / Admin team will ensure that the equipment is tested before installing the same in the work environment.
- For critical servers and equipments, resolution will be performed within the premises and defective item will be sent back. In case the equipment is required to be moved out of the premises, an approval must be taken from the Asset Owner/ IT Manager.
- The Maintenance record will be updated by the IT department with the repair call including the resolution mechanism.

2.3.4 Media Management

- Users will be responsible for protection of Removable Media being used by them and will ensure its storage under lock and key in their absence.
- Users will immediately inform the IT Department in case of hard disk failure along with the sensitivity of information stored on hard disc. In case of any damage to hard disc, IT Department will try to recover data and replace the hard disk.
- Hard disks will be formatted under following conditions:
  - Disposal of old workstations or servers;
  - Issuing workstation or laptop to new users.
- Records of disposal, including time of destruction, name of person who destroyed it and means of disposal will be maintained by the IT Department.
2.3.5 Process for Removal of Equipment / Property

- Formal procedure, standards or guidelines for movement of equipment will be implemented.
- Information processing equipment, information, storage media or software will not be taken off-site without prior authorization from the asset owners or Departmental Head.
- Users who have authority to permit removal of assets will be clearly identified.
- All computer storage media leaving Oil India will be accompanied by an authorized gate-pass and will be logged at designated entry/exit points.
- Gate-passes will clearly indicate if the asset is non-returnable. For all other types of assets time limits for removal will be indicated and returns checked for compliance. Non-compliance must be reported to the IT Department and the Asset Owner.

2.3.6 Process for Returnable Equipments

- IT department will maintain a record of the equipment sent off-premises for repair. At a minimum the following details will be entered in the Outgoing Materials Register:
  - Serial number;
  - Reason for equipment to be sent off-premises;
  - Authorization from approved signatory; and
  - Vendor details including contact name, address and telephone number.
- The IT Department will be responsible for processing a Returnable Gate Pass for the equipment. The IT department is responsible for communicating with the vendor for all ‘Returnable’ equipment. The gate pass will be tracked by the office security personnel.

2.3.7 Disposal or Transfer of Equipments

- Equipment will be disposed (transferred or scrapped) if:
  - The equipment has reached end of life; and
  - The equipment does not suit the environment and support from vendor not available.
OIL-IS-ISMS-AM-Version 1.0 (Asset Management Policy)

- Critical infrastructure equipments which need to be disposed off such as servers, network, security equipments etc. will be approved with valid justification by IT Head and Finance Head. Exceptions to the same can be implemented based on the management approval.
- Any information that resides in the asset will be removed from the equipment before disposal/transfer/scrapping.
- The list of equipments, which are being disposed, will be removed or deleted from Asset list as well as from finance register books.
- List of equipments disposed/ transferred/ scrapped will be maintained separately by the IT Department.

3 Non Compliance

Failure to comply with the Asset Management Policy may, at the full discretion of the Oil India Health, result in disciplinary action as per Information Security Policy.
Document Details

<table>
<thead>
<tr>
<th>Title</th>
<th>Acceptable Usage Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>1.0</td>
</tr>
<tr>
<td>Classification</td>
<td>Internal</td>
</tr>
<tr>
<td>Release Date</td>
<td>01.06.2013</td>
</tr>
<tr>
<td>Description</td>
<td>Acceptable usage of information assets by users</td>
</tr>
<tr>
<td>Update Date</td>
<td>01.06.2013</td>
</tr>
<tr>
<td>Author</td>
<td>CISO</td>
</tr>
<tr>
<td>Reviewer/Custodian</td>
<td>CISO</td>
</tr>
<tr>
<td>Approved By</td>
<td>Information Security Council (ISC)</td>
</tr>
<tr>
<td>Owner</td>
<td>CISO</td>
</tr>
</tbody>
</table>

Distribution List

Name

Internal Distribution Only

Version History

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Version Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>01.06.2013</td>
</tr>
</tbody>
</table>
Table of Contents

1. Purpose .................................................................................................................................4
2. Policy .................................................................................................................................4
  2.1 Application ......................................................................................................................4
  2.2 Personal Use ..................................................................................................................4
  2.3 Monitoring ....................................................................................................................5
  2.4 Archiving ......................................................................................................................5
  2.5 Confidentiality .............................................................................................................5
  2.6 Property .......................................................................................................................6
  2.7 Security ........................................................................................................................6
  2.8 Passwords and Log-in IDs ..........................................................................................6
  2.9 Desktop/Laptop ............................................................................................................7
  2.10 Electronic Games, Jokes and Other Material .............................................................7
  2.11 Prohibited Activities/Use/Communications ...............................................................7
  2.12 Reporting Procedure on Discovery of Policy Violation ................................................10
  2.13 Disclaimer ..................................................................................................................11
  2.14 Good Practice Principle ............................................................................................11
3. Non Compliance .................................................................................................................12
1. Purpose

This Policy supports the high level policy statements defined in Information Security Policy. The purpose of this policy is to clearly illustrate what is considered to be acceptable and unacceptable use of Oil India information systems. The purpose of this policy is to ensure that there is as much clarity as possible about the boundaries of acceptable and unacceptable use of the information assets to which users have access.

2. Policy

2.1 Application

This policy document applies to all Oil India employees, its contractors, its associates and other individuals affiliated with Third Parties who have access to Oil India information resources.

- It is the responsibility of the user to know the guidelines outlined in this policy and to conduct activities accordingly.
- Each user is personally responsible for the control of his/her equipment, including the installed software.

2.2 Personal Use

The primary purpose for the Oil India’s Information systems is for Company business use. Users will make limited, infrequent, or incidental use of Oil India systems for personal use. Personal Use will:

- Adhere to Oil India Security Policies and Guidelines;
- Not interfere with Oil India Business, individual’s productivity, or their colleagues productivity;
- Not adversely affect the Oil India’s ability to provide effective Computer Systems; and
- Not adversely impact on the Oil India’s computing costs.
OIL-IS-POL-AU- 1.0 (Acceptable Usage Policy)

The email system is provided to support the Oil India’s business activities. Personal email, (i.e. communication between individuals or parties which is not in support of the Oil India’s business activities), whilst not prohibited, will be kept to a bare minimum and will be carried out in a manner which does not negatively affect the use of the Oil India’s systems for business purposes.

2.3 Monitoring

- All communications using Company facilities will be the property of Oil India and Oil India reserves the right to access all communications, monitor and audit networks and systems when deemed necessary.

- For security and network maintenance purposes, authorised individuals within Oil India will monitor equipment, systems and network traffic at any time.

- If deemed necessary, content scans will be performed for e-mails sent/received through company systems. E-mail and internet sites that contain certain keywords such as foul language or content that may be of a sexual, pornographic or racist nature will be blocked. In the case of an employee sending inappropriate email or attempted access to blocked internet sites, disciplinary action will be taken.

- E-mails with large attachments that can impact the normal traffic flow will be blocked. Users will be advised not to send such large attachments.

- If an employee has several sent/received mails blocked, the Company will take appropriate measures to ensure such email does not enter the Oil India email system.

2.4 Archiving

The Company will archive all email messages (internal and external) irrespective of their content and store these messages in an archive.

2.5 Confidentiality

- Data created by users on Oil India information systems will be a property of Oil India. Because of the need to protect Oil India network, management cannot guarantee the confidentiality of individual information stored on any network device belonging to the Company.
OIL-IS-POL-AU-1.0 (Acceptable Usage Policy)

- Caution will be exercised over whom users disclose their or a colleague’s email address to, as it can be passed on to unwanted third parties and, thereby, result in unsolicited, unpleasant or abusive email.

- Users will not provide information about, or lists of, Oil India employees to parties outside the Company.

- Information that users consider sensitive or vulnerable will be classified as per the data classification rules and controls will be placed that are apt for such classification.

2.6 Property

- Employees will adhere to all intellectual property and copyright law. Users will always obtain copyright holder’s permission before downloading information from internet or other public computer system.

- No customer related information of any kind and no confidential information regarding any third party will be sent over any public computer system unless the customer or third party have specifically agreed to it.

- All intellectual property rights in computer data, computer files and databases created or altered during the course of employment will be property of Oil India. On termination of employment, users will return all copies of such data, files, and databases in their possession. User will not delete copy of any such computer data, files or databases where that copy is the only, or last remaining, or most up to date copy.

2.7 Security

- Users will inform the security helpdesk of any communication, system problem or other circumstance that may indicate a breach of security or other risk to the integrity of the Company’s information system.

- Users will not circumvent user authentication or security of any host, network or account.

2.8 Passwords and Log-in IDs

- Every user will have a unique login ID and password to access information systems of Oil India. Users will be responsible for setting their passwords as per the Password Management Policy and ensuring that their password is protected.
OIL-IS-POL-AU-1.0 (Acceptable Usage Policy)

- Users will not write down their passwords but protect them by committing them to memory.
- In order to prevent unauthorised use, users will ensure that they do not divulge their password to any other person.
- Users will not disclose password protections or allow any other person access to the Company's information systems.
- Users will not transmit ID's, passwords, internal network configurations or addresses or system names over the Internet.
- Users will not leave their computer unattended while connected to the Internet.

2.9 Desktop/Laptop

To prevent any unauthorized access to personal computers, users will always lock the Desktop/Laptop/Handheld devices when not in use, and set screen savers to require password protection on resume.

- Users will not use Company Computer Systems in any way that may be considered detrimental or offensive to others.
- Any user loading, downloading, printing, storing, or receiving (without reporting to their Manager), any material of a sexual or lewd nature via electronic means or otherwise will be subject to disciplinary action.

2.10 Electronic Games, Jokes and Other Material

Electronic games, jokes, greeting cards, chain letters, non-work related videos and pictures can take up large amounts of server space and adversely impact Company’s Computing Systems. Accessing such material also increases the risk of introducing computer viruses and will thus be considered as a violation of Acceptable Usage Policy.

2.11 Prohibited Activities/Use/Communications

The following activities are prohibited for the users of Oil India information resources. Certain authorized employees may be exempted from some of these restrictions if they are required to perform a particular activity during the course of their legitimate job responsibilities (e.g.
systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). The conduct of any of the activities listed below will be viewed by the Company as misconduct.

- Engaging in any illegal activity (including gambling) while utilising Company information systems.

- Violating the rights of any person or Company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Oil India.

- Copying copyrighted material without authorisation including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music or install any copyrighted software for which Oil India or the end user does not have an active licence.

- Introduction of malicious programs into the network or server (e.g. viruses, worms, Trojan horses, email bombs, etc.) or use the Company’s information systems to transmit malicious programs to other parties.

- Hacking into or obtaining access to any systems or accounts that is not permitted (including systems or accounts outside of the Company) or attempt to do the same or otherwise breach or attempt to breach any computer or network security measures.

- Transmitting (or attempt to transmit) user names, passwords or other information related to the security of the Company's information systems to third parties.

- Using the Company information systems to download, transmit, distribute or process any material which may be considered to be offensive including, without limitation, material which is or may be considered to be racist or sexist, or otherwise discriminatory or to amount to harassment, victimisation or bullying or otherwise to be potentially offensive, upsetting or derogatory to any group or individual or which may be considered to be pornographic, obscene or indecent (in all cases, even if you do not personally consider it to be so).
OIL-IS-POL-AU-1.0 (Acceptable Usage Policy)

- Sending or forwarding threatening, harassing or abusive messages, or any messages that may be construed by the recipient as such, as a result of the language used, frequency of messages received or size of message, font or typeface used (e.g. capitals may be perceived as "shouting" when used in an email) or otherwise.

- Making fraudulent offers of products, items, or services originating from any Oil India account.

- Carrying out or assisting others in carrying out any type of port scan or security scan.

- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

- Providing information about, or lists of, Oil India employees to parties outside the Company.

- Introducing “Dark Objects” or “Dark Shadows” into Oil India computer network. These items are files that could be hidden within the encryption algorithm of any e-mail.

- Loading, downloading, sending, storing, printing or receiving without reporting, offensive, obscene, indecent or defamatory material including any sexual material such as sexually explicit images, messages or cartoons and any material which amounts to harassment or discrimination on the grounds of race, sex or disability.

- Loading, downloading, sending, storing, printing or receiving without deleting, games, jokes, greeting cards, chain letters, executables, non-work related videos and pictures.

- Using another User's login ID and password.

- Changing the configuration of your hardware or software without the prior approval from IT Department except for cosmetic changes such as colour, font, and resolution or display output device.

- Sending or forwarding:
  - Non-business related messages to large numbers of newsgroups e.g. joke, sale items etc.
  - Any material, commentary, opinion or view to any third party which may be defamatory or which may lead to legal proceedings being issued against the Company.
OIL-IS-POL-AU- 1.0 (Acceptable Usage Policy)

- Sending email or other electronic communication that attempts to hide the identity of the sender or represent the sender as someone else or maliciously amend messages received before forwarding that message on to another party.

- Revealing own account password to others or allow use of your account by others. This includes family and other household members when work is being done at home.

- Using or forging email header, footer or disclaimer information for inappropriate or non-business related activities.

- Using the Company information systems for your own personal financial gain or for the financial or business advancement of any third party.

- Posting any information of any kind (including gossip, personal opinions, jokes etc) regarding the Company to any external bulletin board on the Internet.

- Participating in or passing on to any other person any form of chain letter. Any such mail will be deleted as soon as it is received and opened.

- Monitoring or intercepting files or electronic communications of other employees or read, delete, or copy the contents of another person's email mailbox without their consent or appropriate authority.

- Using the email system for personal e-mail subscriptions for non-business activities (e.g. daily joke sites).

2.12 Reporting Procedure on Discovery of Policy Violation

To comply with the Acceptable Systems Use Policy users will follow the below reporting procedure. Failure to report a Policy violation will result in disciplinary action up to and including dismissal.

| Users Who receive or access Material which is offensive, obscene, indecent or defamatory, including any sexual material or any material which | Must Immediately inform the Service Help Desk and the local Human Resources Representative. |
Users Who Must

| amounts to harassment or discrimination on the grounds of race, sex or disability | immediately inform the Service Help Desk |
| receive or access any material, which triggers the computer virus alert software | Immediately delete such items without forwarding on to other parties. |
| receive or access electronic games, jokes, greeting cards, chain letters, executables, non work related videos and pictures | |

2.13 Disclaimer

All external emails from Oil India accounts will carry at minimum the Company details, including name, address, contact details and a disclaimer.

2.14 Good Practice Principle

Oil India Computer System is provided for business use, including electronic communication and the processing of information. Users should always employ good practice principles when using Company Computer Systems. These principles include:

- Treating an e-mail message as if it is a permanent hard copy document to be drafted and checked in the same way. All e-mail messages are permanent records and must be compiled with care.
- Ensuring that all passwords are kept completely confidential.
- Ensuring that any wrongly delivered e-mail messages are immediately recalled and resent to the correct person.
- Avoiding, where possible, sending e-mail messages with large attachments because they can impair the performance of the network.
- Deleting e-mail messages on a regular basis.
OIL-IS-POL-AU-1.0 (Acceptable Usage Policy)

- Scanning any files downloaded from the Internet for viruses before loading or forwarding to other parties.

3. Non Compliance

Failure to comply with the Acceptable Usage Policy may, at the full discretion of Oil India, result in disciplinary action as per Information Technology Policy.
Anti-Virus Policy
Document Number: OIL-IS-POL-AV-1.0
Version : 1.0
# Anti-Virus Policy

**Protection of information systems from all possible computer virus at Oil India**

*Released on 01.06.2013*

## Document Details

<table>
<thead>
<tr>
<th>Title</th>
<th>Anti-Virus Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>1.0</td>
</tr>
<tr>
<td>Classification</td>
<td>Internal</td>
</tr>
<tr>
<td>Release Date</td>
<td>01.06.2013</td>
</tr>
<tr>
<td>Description</td>
<td>Protection of information systems from all possible computer virus at Oil India</td>
</tr>
<tr>
<td>Review Date</td>
<td>01.06.2013</td>
</tr>
<tr>
<td>Author</td>
<td>CISO</td>
</tr>
<tr>
<td>Reviewer/Custodian</td>
<td>CISO</td>
</tr>
<tr>
<td>Approved By</td>
<td>Information Security Council (ISC)</td>
</tr>
<tr>
<td>Owner</td>
<td>CISO</td>
</tr>
</tbody>
</table>

## Distribution List

<table>
<thead>
<tr>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Distribution Only</td>
</tr>
</tbody>
</table>

## Version History

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Version Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>01.06.2013</td>
</tr>
</tbody>
</table>

---

*Internal*
Table of Content

1 Purpose .............................................................................................................................................4
2 Policy ..................................................................................................................................................4
  2.1 Application ....................................................................................................................................4
  2.2 User Responsibility ......................................................................................................................4
  2.3 IT Department Responsibilities ....................................................................................................5
  2.4 Update of Virus ‘Definition’ Files ................................................................................................6
  2.5 Specific Virus protection procedures ............................................................................................6
3 Non Compliance ..................................................................................................................................7
1 Purpose

This Policy supports the high level policy statements defined in Information Security Policy. A computer virus is an unauthorized and malicious program which replicates itself and spreads onto various data storage media across the network such as floppy disk, magnetic disk and tapes. Hence, viruses are a threat to the integrity and availability of data/information and can prove very harmful to an organization in terms of lost data, lost staff productivity, and/or lost reputation. The purpose of this policy is to develop and implement systems and procedures for Oil India for protection of its IT systems from all possible computer virus.

2 Policy

2.1 Application

This policy document applies to all employees, including full-time staff, part-time staff, contractors, freelancers, and other agents who have access to Oil India’s computer systems and/or Network. The policy also defines procedures to be implemented to ensure all servers and computer systems are updated with Company’s standard anti-virus program with latest virus definition file.

Further, this policy applies to all systems that are connected to the Oil India network via a standard network connection, wireless connection, modem connection and/or virtual private network connection.

2.2 User Responsibility

- Upon encountering a virus attack, users will immediately stop using the involved desktop/laptop and/or any other computer system and report it to Service Desk.
- Users will not attempt to destroy or remove a virus, or any evidence of that virus, without directions from the IT department.
- Users will not open any files attached to an email from an unknown, suspicious or untrustworthy source.
- User will scan every diskette, CD and DAT tape before use.
Users will delete chain and junk emails and not forward or reply to any of them. These types of email are considered spam, which is unsolicited, intrusive mail that clogs up the network.

If instructed to delete e-mail messages believed to contain a virus, users will ensure that the message is deleted from Deleted Items and Trash folder as well.

Users will exercise caution when downloading files from the Internet and ensure that the source is a legitimate and reputable one.

User will check whether updated antivirus definition file is as current as maximum one week. In case it is older than one week user will raise ticket with IT helpdesk.

User will not stop the scheduled antivirus scanning or alter the setting of Antivirus client.

User will not un-install Antivirus software provided by OIL and install any other Antivirus software.

Users will back up the files on a regular basis. If a virus destroys the data files, they can be replaced with the back-up copy.

When in doubt, users will not open, download, or execute any files or email attachments.

Users will not perform direct disk sharing with read-write access unless approved by the IT Department.

2.3 IT Department Responsibilities

Ensure all servers, desktops and laptops are installed with company standard Anti-Virus Program. Proper password protection settings are available so that the Anti-virus check cannot be disabled by the users.

Provide newer versions/engines of Anti-virus programs in regular and timely manner and ensure a quick roll-out across the organization.

Ensure all Servers and PCs are updated with latest Virus Definition file.

Ensure anti-virus software run at least once in a week and are properly scheduled, preferably during the lunch hours/off hours of the office.

Ensure every diskette and DAT tape is scanned for virus before use.

Review and update the Anti-Virus Policy and upload it on the intranet.
• Automatic antivirus scanning option is enabled for any files that are restored to Company’s production computer system

• All the servers will be installed with the Antivirus software before it is assigned for a specific function.

• The software used will be from the original media obtained from the vendor or downloaded from their official website.

2.4 Update of Virus ‘Definition’ Files

These are the files, which contain the virus signatures. Following policies will be followed to maintain updated ‘Definition’ files:

• The IT Department will keep the updated virus signatures on the central host server;

• Operating system job will be scheduled in the network server for pushing the DAT file updates onto client computers /network nodes connected on daily basis; and

• All emergency virus update files will be pushed to the client computers -network nodes immediately.

2.5 Specific Virus protection procedures

• Software/data downloaded from outside sources such as Internet may contain a virus.

• The most current available version of the anti-virus software package will be taken as the default standard.

• Scheduler will be configured to run the Anti Virus software at least once a week. Users will not be allowed to stop the Anti-virus check.

• Appropriate protection will be enforced so that the users cannot disable the Anti-virus check.

• Upon encountering the virus problem, the AV software will clean the infected files and if fails will delete the file. The other options such as ‘continue’ and ‘move to a directory’ in AV check will not be enabled.
**OIL-IS-POL-AV-1.0 (Anti-Virus Policy)**

- The floppy drives of all desktops/laptops will be disabled unless and until there exists a valid business justification. Approval for the same will be taken from the IT Department and Functional Manager by providing valid business justification.

- User desktops/laptops will not be configured for any shares. This will restrict the spread of virus to other systems to an extent. All the data that needs to be shared will be stored on a dedicated server from which users can retrieve/store their data.

- Virus logs utility in Anti-Virus check software will always be enabled and the logs will be reviewed by Systems Engineer. The logs will be configured to display virus identity (if any) so that the IT team can subsequently update its software to detect new viruses as well as mutated versions of old viruses.

### 3 Non Compliance

Failure to comply with the Anti-Virus Policy may, at the full discretion of the Oil India, result in disciplinary action as per Information Security Policy.
 Describe business continuity management policy details and version history.

---

### Document Details

<table>
<thead>
<tr>
<th></th>
<th>Signatures with Date</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Title</strong></td>
<td>Business Continuity Management Policy</td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>1.0</td>
</tr>
<tr>
<td><strong>Classification</strong></td>
<td>Internal</td>
</tr>
<tr>
<td><strong>Release Date</strong></td>
<td>01.06.2013</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Develop a continuity plan for timely resumption of business activities to minimize losses</td>
</tr>
<tr>
<td><strong>Update Date</strong></td>
<td>01.06.2013</td>
</tr>
<tr>
<td><strong>Author</strong></td>
<td>CISO</td>
</tr>
<tr>
<td><strong>Reviewer/ Custodian</strong></td>
<td>CISO</td>
</tr>
<tr>
<td><strong>Approved By</strong></td>
<td>Information Security Council (ISC)</td>
</tr>
<tr>
<td><strong>Owner</strong></td>
<td>CISO</td>
</tr>
</tbody>
</table>

### Distribution List

<table>
<thead>
<tr>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Distribution Only</td>
</tr>
</tbody>
</table>

### Version History

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Version Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>01.06.2013</td>
</tr>
</tbody>
</table>
Table of Content

1. Purpose ...................................................................................................................... 4
2. Policy .......................................................................................................................... 4
2.1. Application ................................................................................................................. 4
3. Key Practices and Responsibilities ............................................................................. 4
4. Key Practice Details .................................................................................................... 5
4.1 Information Security Aspects of Business Continuity Management ....................... 5
4.2 Business Continuity and Risk Assessment ........................................................................ 6
4.3 Developing and implementing continuity plans including information security ...... 7
4.4 Business Continuity Planning Framework .................................................................. 7
4.5 Testing, Maintenance and Reassessing Business Continuity Plan ............................. 8
4.6 Crisis Management .................................................................................................... 9
1. **Purpose**

This Policy supports the high level policy statements defined in Information Security Policy. The purpose of this policy is to implement a process of risk and business impact analysis of major failures or disasters resulting in loss of resources supporting the business processes; Mitigate the risk of interruptions to business activities from the effects of such major failures or disasters; and Develop a continuity plan and implement the controls to mitigate the impact of disaster and timely resumption of business activities to minimize losses.

2. **Policy**

2.1. **Application**

This policy document applies to All Oil India employees, its contractors, its associates and other individuals affiliated with Third Parties who have access to Oil India information resources which includes computers whether server or client, all network equipment, infrastructure equipment, operating systems, messaging systems, software, output devices and storage mediums. All information assets owned or managed by Oil India including systems owned (if any) by outsourcing vendors and third parties used for processing Oil India information.

3. **Key Practices and Responsibilities**

The key practices and responsibilities are as follows:

<table>
<thead>
<tr>
<th>S.No</th>
<th>Key Practice</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Development and Maintenance of the business continuity plan</td>
<td>Information Security Council (ISC)</td>
</tr>
<tr>
<td>2.</td>
<td>Availability and timely recovery of identified business processes</td>
<td>CISO</td>
</tr>
<tr>
<td>3.</td>
<td>Ensuring that all personnel are trained</td>
<td>CISO</td>
</tr>
<tr>
<td>4.</td>
<td>Managing the contingencies in their respective processes.</td>
<td>Individual process owners</td>
</tr>
</tbody>
</table>
4. **Key Practice Details**

4.1 **Information Security Aspects of Business Continuity Management**

A managed process for development and maintenance of business continuity will exist throughout the organization. The following key components of Business Continuity Management will be considered:

- Identification of critical business processes;
- Risk assessment and Business impact analysis;
- Preparation of Business Continuity Plan (BCP) (including Disaster Recovery Plan, Business Resumption Plan and Crisis Management Program); and
- Regular testing and maintenance of BCP.

The business continuity management cycle at Oil India shall be as below:
4.2 Business Continuity and Risk Assessment

- The management will conduct a formal risk assessment and business impact analysis to determine the requirements of BCP. Respective functional teams will conduct the impact analysis and identify the causal threats and assess the impact keeping in view the classification of information assets within the process. Risk will be assessed as a function of the threat probability and business impact while:
  - developing the business continuity plan; and
  - reviewing and updating the business continuity plan (once a year)
Business impact analysis will be carried out to evaluate the acceptable downtime of all the critical business application systems & processes and their impact on the business.

The maximum acceptable downtime for the business systems and processes will be documented in the BCP.

Risk and business impact assessment will be reported by the process owners to the Information Security Council (ISC).

4.3 Developing and implementing continuity plans including information security

Business continuity plans will be developed based on the risks faced by the organization. The BCP will assist in counteracting interruptions to business activities, to protect critical business processes from the effects of major failures or disasters, and to continue business operations during contingency period.

The coverage of continuity plans will enable business operations to be maintained following failure or damage of vital services or facilities.

4.4 Business Continuity Planning Framework

A single common framework shall be followed for drafting continuity plans as per business requirements, which will include the key stakeholders, including third parties. The risks and business impacts shall be considered for developing and updating the business continuity strategy of the company. The framework shall include but not be limited to:

- Establishing recovery time objectives;
- Type of disruption;
- Conditions for disaster declaration and plan invocation;
OIL-IS-POL-BCM-1.0 (Business Continuity Management Policy)

- Disaster Recovery Plan: A plan that describes the process to recover from major processing interruptions;
- Business Resumption Plan: A plan to ensure the continued availability of essential services, programs and operations in the event of a disaster;
- Crisis Management Program: A program to identify the potential crisis and planning a response to the crisis and, confronting and resolving the crisis; and
- Testing and maintenance program.

• The plan will include established emergency procedures, existing fallback arrangements for computer services, telecommunications and accommodation/facilities. Further, each plan will specify the conditions for activating the plan and the individuals responsible for executing the plan. Also, the plan will include business resumption (migration) procedures, and a test schedule for the plan.

• BCP will be issued to identified and authorized personnel only. Adequate education activities will have to be conducted to create understanding and awareness about the business continuity plan.

• BCP will include the roles and responsibilities to be performed by the contingency team members, in the event of a contingency.

• Awareness and education activities will be carried out for creating the understanding of the business continuity process.

4.5 Testing, Maintenance and Reassessing Business Continuity Plan

• The BCP will be tested on a yearly basis to ensure the practicability and workability of the plan. Further, the plan will be reviewed on a yearly basis, and updated to reflect all the changes in the identified critical business processes.
• Formal change control mechanisms will be in place to ensure that implications of change are identified and disseminated prior to update and redistribution of plans.

4.6 Crisis Management

Business continuity plan shall comprise of a crisis management program including but not limited to contain:

• List of command centers (emergency command center);

• Directions to the alternate sites and muster points;

• Emergency response procedures (during and after normal business hours);

• Communication procedures, including but not limited to crisis management team, strategic outsourced partners, third parties;

• Appropriate references to human resource policies for meeting crisis requirements;

• Executive succession; and

• Controls for access to BCP.
Backup Management Policy

Document Number: OIL-IS-POL-BM-1.0

Version: 1.0
## Document Details

<table>
<thead>
<tr>
<th></th>
<th>Signatures with Date</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Title</strong></td>
<td>Backup Management Policy</td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>1.0</td>
</tr>
<tr>
<td><strong>Classification</strong></td>
<td>Internal</td>
</tr>
<tr>
<td><strong>Release Date</strong></td>
<td>01.06.2013</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Backup and restoration of critical information in Oil India</td>
</tr>
<tr>
<td><strong>Review Date</strong></td>
<td>01.06.2013</td>
</tr>
<tr>
<td><strong>Author</strong></td>
<td>CISO</td>
</tr>
<tr>
<td><strong>Reviewer/Custodian</strong></td>
<td>CISO</td>
</tr>
<tr>
<td><strong>Approved By</strong></td>
<td>Information Security Council (ISC)</td>
</tr>
<tr>
<td><strong>Owner</strong></td>
<td>CISO</td>
</tr>
</tbody>
</table>

## Distribution List

<table>
<thead>
<tr>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Distribution Only</td>
</tr>
</tbody>
</table>

## Version History

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Version Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>01.06.2013</td>
</tr>
</tbody>
</table>
# Table of Content

1. **Purpose** ...................................................................................................................... 4  
2. **Policy** .......................................................................................................................... 4  
   2.1. **Application** ........................................................................................................... 4  
   2.2. **Backup Types & Planning** .................................................................................... 4  
   2.3. **Backup Logging and Audit Trail** ......................................................................... 5  
   2.4. **Backup Storage** ................................................................................................... 6  
   2.5. **Backup Restoration and Testing** ......................................................................... 6  
3. **Non Compliance** ........................................................................................................ 7
1. Purpose

This Policy supports the high level policy statements defined in Information Security Policy. In order to safeguard information and computing resources from various business and environmental threats, systems and procedures need to be developed and implemented for backup of all business data, related application systems and operating systems software. The purpose of the Backup Management Policy is to ensure that the critical information assets of Oil India are backed-up and are recoverable as and when required. This would also ensure that all backups of information assets are in accordance with the approved business and technical requirements and are planned, implemented and tested in a controlled and consistent manner.

2. Policy

2.1. Application

This policy document applies to all information and information assets at Oil India available with Oil India employees, including full-time staff, part-time staff, contractors, freelancers, and other agents, which includes corporate data, business applications and system software.

2.2. Backup Types & Planning

- All company critical information will be backed up and tested for restoration to ensure availability of such information as required.
- Information will be backed up as per its classification.
- IT Department will maintain a documented Backup plan for all the information and information assets identified to be backed up. The plan will include:
  - Information to be backed up;
  - name of the system hosting the information (e.g. server name);
  - Supporting IT infrastructure details hosting the information (e.g. server hardware details);
  - The type of backup – i.e. online/offline, incremental/full etc.
OIL-IS-POL-BM-1.0 (Backup Management Policy)

− Backup periodicity – daily, weekly, monthly, annual based on the criticality of information; and
− Retention period of the data and offsite storage location if required.

• IT systems will be backed-up in two ways – scheduled and unscheduled. While the former will be done at a defined frequency, the latter are ad hoc in nature and will be performed as and when required.

• The information owners will formally intimate the IT Department about any new applications and its data to be backed up. Similarly, the IT Department will be informed about discontinuing the backup of the applications systems no longer in use.

• Retention period for unscheduled backup will be defined and the tapes will get adequately stored.

• Backup media will be regularly examined for readability of the data. The backup media will be replaced immediately after encountering an error or at predefined time intervals whichever is earlier.

• Unscheduled backups will be stored for the time period as defined by the requester.

• IT Department will be responsible for the implementation of the backup plan for production servers.

• Information custodian will be responsible for ensuring the successful backup of the information assets as per the backup plan defined.

2.3. Backup Logging and Audit Trail

• Backup logs will be recorded for all the backups taken and will be reviewed periodically.

• A “Backup Checklist” will be maintained to include, but not limited to, the following details:
  − the application / server for which the backup has been taken;
  − start and finish times;
  − the label of the media on which the backup had been taken;
  − the Status of the Backup – Successful/ Unsuccessful/ Incomplete; and
  − sign offs from the personnel responsible for taking the Backup and personnel approving the successful completion of the planned backup.
Backup failures will be treated as incidents and will be handled as per the Incident Management Policy.

2.4. Backup Storage

- Backup tapes will be “write-protected” to prevent accidental overwriting.
- Critical backup tapes will be sent offsite as per frequency specified in the backup plan. These tapes will be stored in a fire proof cabinet at the offsite location as well.
- The list of tapes going offsite and the tapes coming from the offsite location will be documented.

2.5. Backup Restoration and Testing

- Personnel requiring files to be restored from backup will submit a request authorized by the supervisor/ function head and IT Head to IT Department. Upon receiving authorization, data will be restored by the IT Department.
- A Backup Restoration Log will be maintained to include, but not limited to, the following details:
  - date for data recovery;
  - start and end times of recovery;
  - personnel requesting the data recovery;
  - personnel responsible for the recovery;
  - reason for data recovery; and
  - status.
- Restoration testing will be performed on quarterly basis. A tape will be selected at random by the IT Department and the full contents of the tape will be restored.
- The restored contents will be verified against the tape for an exact match. This will be verified by IT Head.
- The entire restoration process will be documented detailing the test plan, the procedures executed and the test results.
3. Non Compliance

Failure to comply with the Backup Management Policy may, at the full discretion of the Oil India, result in disciplinary action as per Information Security Policy.
Clear Desk and Clear Screen Policy

Document Number: OIL-IS-POL-CDCS-1.0 (Clear Desk & Clear Screen Policy)

Version : 1.0

Oil India Limited
(A Government of India Enterprise)
To reduce the risk of unauthorized access, loss of, and damage to information during and outside normal working hours by unauthorized personnel having physical access to the workstation-workplace.
Table of Contents

1. Purpose ...................................................................................................................... 4
2. Policy .......................................................................................................................... 4
2.1 Application ................................................................................................................. 4
2.2 Users’ Responsibilities ............................................................................................. 4
3. Clear desk policy ......................................................................................................... 4
4. Clear screen policy ..................................................................................................... 5
5. Non Compliance ......................................................................................................... 5
1. Purpose

This Policy supports the high level policy statements defined in Information Security Policy. A clear desk-clear screen policy reduces the risks of unauthorized access, loss of, and damage to information during and outside normal working hours. Use of safes and other forms of secure storage facilities, as stipulated by the policy, also offers protection to information stored therein against disasters such as a fire, earthquake, flood or explosions.

2. Policy

2.1 Application

This policy document applies to all Oil India employees, its contractors, its associates and other individuals affiliated with Third Parties who have access to Oil India information resources which includes computers whether server or client, all network equipment, infrastructure equipment, operating systems, messaging systems, software, output devices and storage mediums.

2.2 Users’ Responsibilities

Employees will keep information assets like documents correspondence, computer media, etc. in a secured place when not in use, especially after working hours. Users will protect personal computers and terminals with adequate controls (workstation locks, passwords, etc) when not in use and will shut down desktops when leaving the office

3. Clear desk policy

– All sensitive information will be kept in a secure office or other location e.g. storage in a locked drawer, file cabinet etc.

– All non-public documents when printed or scanned will be cleared from printers or scanners.
OIL-IS-POL-CDCS-1.0 (Clear Desk and Clear Screen Policy)

- All incoming and outgoing mail points and unattended facsimile machines will be protected from unauthorized physical and logical access.
- Unauthorized use of photocopier and other reproduction technologies (e.g. scanners, digital cameras etc.) will be prevented.

4. Clear screen policy

- Personal computers, computer terminals and printers will be left logged off or protected with a screen and keyboard locking mechanism controlled by a password, token or similar user authentication mechanism when unattended.
- Password-protected screen savers will be activated within 5 minutes of user inactivity.
- Users will log off or lock their personal computers when leaving it unattended for any period of time.
- Users will turn off personal computers or log off all network resources at the end of each day.

5. Non Compliance

Failure to comply with the Clear Desk and Clear Screen Policy may, at the full discretion of the Oil India, result in disciplinary action as per Information Security Policy.
Change Management Policy

Document Number: OIL-IS-POL-CM-Version 1.0
Version : Version 1.0
OIL-IS-POL-CM-Version 1.0 (Change Management Policy)

Document Details

<table>
<thead>
<tr>
<th>Title</th>
<th>Change Management Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Version 1.0</td>
</tr>
<tr>
<td>Classification</td>
<td>Internal</td>
</tr>
<tr>
<td>Release Date</td>
<td>01.06.2013</td>
</tr>
<tr>
<td>Description</td>
<td>Efficient and prompt handling of all changes to minimize the impact of change</td>
</tr>
<tr>
<td>Review Date</td>
<td>01.06.2013</td>
</tr>
<tr>
<td>Author</td>
<td>CISO</td>
</tr>
<tr>
<td>Reviewer/Custodian</td>
<td>CISO</td>
</tr>
<tr>
<td>Approved By</td>
<td>Information Security Council (ISC)</td>
</tr>
<tr>
<td>Owner</td>
<td>CISO</td>
</tr>
</tbody>
</table>

Distribution List

Name

Internal Distribution Only

Version History

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Version Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 1.0</td>
<td>01.06.2013</td>
</tr>
</tbody>
</table>
Table of Contents

1. Purpose ...................................................................................................................... 4
2. Policy .......................................................................................................................... 4
2.1 Application ................................................................................................................. 4
2.2 Change Initiation ........................................................................................................ 4
2.3 Change Analysis ....................................................................................................... 5
2.4 Change Approval ..................................................................................................... 7
2.5 Implementing Change Request .................................................................................. 7
2.6 Emergency Changes ............................................................................................... 9
2.7 Rescheduling Changes ........................................................................................... 9
3. Non Compliance ....................................................................................................... 10
1. Purpose

This Policy supports the high level policy statements defined in Information Security Policy. The purpose of the policy is to set up formal controls for executing and monitoring the changes to Hardware, System and Subsystem software, Application software/Enabling applications, Configurations (Physical and Logical), Network and Facilities in order to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes, to minimize the impact of change-related incidents upon service quality, and consequently to improve the day-to-day operations of the organization.

2. Policy

2.1 Application

This policy applies to employees, including full-time staff, part-time staff, contractors, freelancers, and other agents of Oil India’s application development team, and all application development team information resources as well as the application, systems software and infrastructure deployed.

2.2 Change Initiation

- All change requests will be routed to IT Managers identified in the IT Department.

- Change request procedure will be initiated by requesting for a change with the requirements specified in a Change Request Form (CRF) to the IT Managers.

- The change request will at least include the following:
  - Affected Asset Name;
  - Change Description;
  - Reason for Change;
  - Business impact of the change;
− Expected date of completion;
− IT Manager/ Application Owner approval; and
− Comments (if any).

• The requestors for the changes will be as follows:
  − Network changes will be raised by the network administrator;
  − Operating system changes will be raised by the system administrator;
  − Security configuration changes will be raised by the network and security administrator; and
  − Application changes will be raised by OIL India software team.
  − End users will raise change requests for specific requirements pertaining to their projects or functions and the applications used by the end users.

• The IT service desk will:
  − Assign a Change Request Number to the request and record it in the Change Management Register; and
  − Assign the change request to an IT team member who will log the request details in the change management register.

• If the change is classified as emergency change, Emergency change process will be initiated as per the Emergency Change Management Procedure immediately.

2.3 Change Analysis

• The assigned team member will perform requirements gathering and impact analysis of the change and update the following in the details in the CRF:
  − Urgency of change
    ○ Critical(C3)
    ○ High(C2)
**OIL-IS-POL-CM-Version 1.0 (Change Management Policy)**

- Medium(C1)
- Low(C0)
  - Impact of change
    - Extensive/ Widespread
    - Significant/ Large
    - Moderate/ Limited
    - Minor/ Localised
  - Priority (Impact and Urgency) of change
    - Critical
    - High
    - Medium
    - Low
  - Functional specifications (to be populated based on requirement gathering from the requestor);
  - Technical specifications;
  - Impact analysis;
  - Test scenarios;
  - Resources/costs involved (if any);
  - Downtime requirements (if any);
  - Key Stakeholders likely to be affected due to the change; and
  - Fall-back plan.

- The assigned team member will determine whether the changes compromise the security controls implemented for the IT Systems / Network. In such cases, approval will be obtained from Chief Information Security Officer prior to initiating the change resolution.


**Oil India Limited**

_OIL-IS-POL-CM-Version 1.0 (Change Management Policy)_

- Turnaround times will be defined for all types of changes and updated in the change request form. The turnaround time is calculated from the time the change request is submitted, to the scheduled implementation date.

### 2.4 Change Approval

- Approval matrix will be defined for all types of changes depending upon priority and risk. All changes will require approvals as per the approval matrix.
- No change will be approved by the requester or implementer of the change.

### 2.5 Implementing Change Request

- The assigned IT Team member will develop the change on the test environment (if development is not possible).
- Testing will be performed based on the test scenarios developed and the test results will be documented. For critical fixes no testing is performed, directly it is moved to implementation platform.
- After every stage of change, the outcome will be tested. If the outcome is not as expected, then the change will be stopped immediately and IT Head will be informed. After consultation with the manager, the change executor will either execute the fallback procedure for the change or if the risk is low and warning can be ignored.
- Testing will not be performed by the change developer.
- Once the system testing is successful in test environment, the client server will be made available for the user to perform user acceptance testing (if applicable). The user acceptance of the change will be recorded in the CRF.
- Executable codes will be ported to production environment after successful testing.
- IT Administrator will maintain previous versions of software or configuration files.
- Backup of the database will be taken before copying the change to production or live environment.
- Fallback procedures will be defined for the changes to be implemented to go back to original state in case of change failure.
For changes requiring downtime, all stakeholders will be informed in advance of the system unavailability. The IT Team will try to execute the changes with minimum impact on business activity.

Change executor will not cross the agreed time schedule, if there is chance of change getting spilled over then it will be immediately informed to IT Manager.

Post introduction of the change, the assigned team member will mention the actual completion time and downtime taken to perform the change as well attach the test results in the CRF.

The complete CRF will be submitted to Change Approver on successful completion of change.

The IT Department will maintain the system documentation of the changes. It will be ensured that the user operating manual as well as system documentation is updated on a timely basis.

Vendor supplied product will be used without modification. If this is unavoidable then concerned vendors will be requested to make required changes as a standard program update.

The change documentation will contain at least:

- Priority;
- Brief Description;
- Time of Change;
- Duration of Change;
- Impact assessment and any outage required;
- Implementation Plan;
- Fallback procedures;
- Name and Position of person executing the change;
- Name and Position of person managing the change; and
- Name and Position of person signing off completion.
2.6 Emergency Changes

Emergency change control will be used to remedy extraordinary circumstances that cannot otherwise be resolved in the course of normal business activities without significant impact on the business.

- Verbal approvals will be obtained from the IT Application Owner/ IT Infrastructure Manager before implementing an emergency change.

- Change implementation process as specified above (as per section 2.5 implementing change request) will be followed for implementing emergency changes.

- Once the change has been implemented successfully, the IT Application Owner/ IT Infrastructure Manager will ensure that all activities performed for the emergency changes are documented. This documentation will include all the details required for a normal change (as per section 2.5 implementing change request).

- Any sub-normal procedures followed during the emergency program change (e.g. giving super-user or root password to the support personnel performing trouble-shooting etc.) will be identified and restored to the original settings and configurations.

- Even in the situation of an emergency, the ‘need-to-do’ principle will be followed, with appropriate restrictions on the support personnel executing program changes.

2.7 Rescheduling Changes

- Rescheduling of changes will be carried out under following circumstances:
  - Change in implementation plans/additional information requirement etc. during approval stage;
  - Conflicting change is identified;
  - Downtime is required outside scheduled maintenance window; and
  - Change needs to be backed out & rescheduled.

- All the approvals will be obtained again before implementing a rescheduled change.
3. Non Compliance

Failure to comply with the Change Management policy may, at the full discretion of the Oil India, result in the suspension of any or all remote access privileges, disciplinary action, and possibly termination of employment.
Disciplinary Action Policy
Document Number: OIL-IS-POL-DA-1.0
Version : 1.0
Document Details

<table>
<thead>
<tr>
<th></th>
<th>Signatures with Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Disciplinary Action Policy</td>
</tr>
<tr>
<td>Version</td>
<td>1.0</td>
</tr>
<tr>
<td>Classification</td>
<td>Internal</td>
</tr>
<tr>
<td>Release Date</td>
<td>30.05.2013</td>
</tr>
<tr>
<td>Description</td>
<td>Disciplinary action policy</td>
</tr>
<tr>
<td>Update Date</td>
<td>30.05.2013</td>
</tr>
<tr>
<td>Author</td>
<td>Oil India Ltd</td>
</tr>
<tr>
<td>Reviewer/Custodian</td>
<td>Naba Jyoti Neog</td>
</tr>
<tr>
<td>Approved By</td>
<td>Information security Council (ISC)</td>
</tr>
<tr>
<td>Owner</td>
<td>IT Department, OIL</td>
</tr>
</tbody>
</table>

Distribution List

<table>
<thead>
<tr>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td>Internal Distribution Only</td>
</tr>
</tbody>
</table>

Version History

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Version Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Draft 0.1</td>
<td></td>
</tr>
<tr>
<td>1.0</td>
<td>30.05.2013</td>
</tr>
</tbody>
</table>
# Table of Contents

1. **Purpose** ...................................................................................................................... 4
2. **Policy** .......................................................................................................................... 4
   2.1 **Scope** .................................................................................................................. 4
   2.2 **Introduction** ......................................................................................................... 4
   2.3 **Guidelines for Offence Categorization** ............................................................... 5
   2.4 **Disciplinary Action** ............................................................................................. 7
3. **Non Compliance** ....................................................................................................... 7
1. **Purpose**

This Policy supports the high level policy statements defined in Information Security Policy. The purpose of this policy is to detail the disciplinary action policy for Oil India.

2. **Policy**

2.1 **Scope**

This policy is applicable to all employees and third party vendor staff of Oil India.

2.2 **Introduction**

Employees and third party staff at Oil India are expected to comply with and abide by all the policies, guidelines, rules and agreements as amended from time to time. In the eventuality of (a) breach of any of the policies, guidelines, rules and agreements; (b) misconduct and; (c) non-performance by any employee of Oil India, Disciplinary Action Policy will be initiated.

Discipline is action that corrects or improves. Its purpose in the workplace is to correct or improve job-related performance or behavior. At Oil India most workplace performance problems shall be handled by informal discussion and counseling between the supervisor and the employee. This policy shall be applied when more formal action is required.

**Third Party Staff:**

In case of third parties’ staff breach of agreement, misconduct and non-performance, Oil India Management Committee will have the sole discretion to initiate disciplinary action in consultation with Legal, Personnel and any other concerned departments. This could vary from being a verbal warning to the third party vendor to termination of services of the vendor or even legal proceedings, as the case maybe.

The rest of this policy focuses on the disciplinary action policy for employees.
2.3 Guidelines for Offence Categorization

These guidelines provide guidance in categorizing an observed or reported offence according to specific severity so as to take effective disciplinary action. These guidelines should be used by concerned authority involved in deciding on the disciplinary action.

Indicative categorization of the security incidents is provided in the table below:

<table>
<thead>
<tr>
<th>Type of violation</th>
<th>High</th>
<th>Severity Medium</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Physical Security at IT Data Center</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Making or allowing an unauthorized entry into restricted areas like IT Data centre</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Entry into premises without identification badges</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>3. Piggybacking/ tailgating in the premises</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>4. Smoking, eating or drinking in the server room</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>5. Improper handling of diskettes, tapes, etc.</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>(e.g., bringing magnetic material near such storage media, not ensuring proper atmospheric conditions for their storage, etc.)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Unauthorized removal of equipment from the premises</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Unauthorized relocation of equipment inside the premises</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>8. Leaving laptops in insecure areas (i.e., unlocked cabinets)</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>9. Non-adherence to environmental precautions for server room</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td><strong>E-Mail Security</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10. Unauthorized use of another person’s e-mail</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11. Knowingly sending viruses through e-mail attachments</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12. Inappropriate auto forwarding of e-mail</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>13. Using e-mail in a manner that:</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>• interferes with normal business activities or hampers employee productivity;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• embarrasses Oil India;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• consumes more resources;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• involves solicitation;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• is associated with any for-profit outside business activity.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### OIL-IS-POL-DA-1.0 (Disciplinary Action Policy)

<table>
<thead>
<tr>
<th>Type of violation</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>High</strong></td>
<td><strong>Medium</strong></td>
</tr>
<tr>
<td>14 Blanket forwarding of e-mail</td>
<td>X</td>
</tr>
<tr>
<td>15 Sending profane, obscene or derogatory e-mails</td>
<td>X</td>
</tr>
<tr>
<td><strong>Passwords</strong></td>
<td></td>
</tr>
<tr>
<td>16 Violating password usage conventions</td>
<td>X</td>
</tr>
<tr>
<td>17 Password sharing / disclosure for secret/confidential or highly sensitive information assets</td>
<td>X</td>
</tr>
<tr>
<td>18 Insecure storage of critical passwords</td>
<td>X</td>
</tr>
<tr>
<td>19 Requesting / making unauthorized password resets of other users</td>
<td>X</td>
</tr>
<tr>
<td>20 Requesting / making password resets of other users in their absence for emergency business purposes without appropriate approval</td>
<td>X</td>
</tr>
<tr>
<td>21 Non-use of screen saver / power-on passwords on user desktops</td>
<td>X</td>
</tr>
<tr>
<td>22 Non-use of screen saver / power-on passwords on server consoles</td>
<td>X</td>
</tr>
<tr>
<td>23 Not disabling default passwords</td>
<td>X</td>
</tr>
<tr>
<td>24 Sharing of passwords by end users</td>
<td>X</td>
</tr>
</tbody>
</table>

The following, while not all-inclusive, are examples of some behaviour that may be subject to accelerated Disciplinary Action:

- Integrity policy violation;
- Fraud / Embezzlement / Theft;
- Falsification of records;
- Threatening or acts of violence at the workplace;
- Breach of confidentiality;
- Substance/ alcohol abuse at workplace;
- Improper use of company equipment/ misuse of company guidelines;
- Workplace harassment;
- Excessive absenteeism; and
OIL-IS-POL-DA-1.0 (Disciplinary Action Policy)

- Discrimination based on caste, religion etc.

2.4 Disciplinary Action

Security Incidents as described in Section 2.3 shall be considered as Misconduct and shall be dealt with rules and procedures of existing Oil Executives' Conduct, Discipline and Appeal Rules and modified standing Order.

3. Non Compliance

All employees are required to read the disciplinary action policy.
**Document Details**

<table>
<thead>
<tr>
<th>Title</th>
<th>Data Classification Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Version 1.0</td>
</tr>
<tr>
<td>Classification</td>
<td>Internal</td>
</tr>
<tr>
<td>Release Date</td>
<td>01.06.2013</td>
</tr>
<tr>
<td>Description</td>
<td>Ensures that information is disclosed only to those people who have a legitimate business need for the information and is protected in a manner commensurate with its sensitivity</td>
</tr>
<tr>
<td>Review Date</td>
<td>01.06.2013</td>
</tr>
<tr>
<td>Author</td>
<td>CISO</td>
</tr>
<tr>
<td>Reviewer-Custodian</td>
<td>CISO</td>
</tr>
<tr>
<td>Approved By</td>
<td>Information Security Council (ISC)</td>
</tr>
<tr>
<td>Owner</td>
<td>CISO</td>
</tr>
</tbody>
</table>

**Distribution List**

<table>
<thead>
<tr>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Distribution Only</td>
</tr>
</tbody>
</table>

**Version History**

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Version Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 1.0</td>
<td>01.06.2013</td>
</tr>
</tbody>
</table>
Table of Contents

1. Purpose ...................................................................................................................... 4
2. Policy .......................................................................................................................... 4
2.1. Application ................................................................................................................. 4
2.2. Classification of Data ................................................................................................. 4
   2.2.1. Restricted ................................................................................................................. 5
   2.2.2. Confidential .............................................................................................................. 5
   2.2.3. Internal ..................................................................................................................... 5
   2.2.4. Public ........................................................................................................................ 5
2.3. Pre-Conditions - Rules for Data Classification ....................................................... 6
2.4. Cumulative Classification ......................................................................................... 6
2.5. Reclassification - Declassification ........................................................................... 6
3. Non Compliance ......................................................................................................... 7
1. Purpose

This Policy supports the high level policy statements defined in Information Security Policy. Information is a critical resource for an organization and needs to be protected throughout its lifecycle from unauthorized disclosure, use, modification, and deletion. To achieve this, information must be made accessible on “need-to know” basis. The purpose of this document is to provide overall policy on data classification to the organization, which includes protection of information from unauthorized generation, access, modification, disclosure, transmission or destruction. The policy ensures that information is disclosed only to those people who have a legitimate business need for the information and is protected in a manner commensurate with its sensitivity, no matter where it resides, what form it takes, what technology is used to handle it, and what purpose it serves.

2. Policy

2.1. Application

This policy is applicable to all employees, including full-time staff, part-time staff, contractors, freelancers, and other agents who have access to any information asset (both hardcopy and softcopy) at Oil India. This data classification scheme is applicable to all information, whether stored or transmitted, which is in the possession or under the control of Oil India.

2.2. Classification of Data

All the information assets in Oil India will be classified under the following categories as described below:

- Restricted
- Confidential
- Internal
OIL-IS-POL-DC-Version 1.0 (Data Classification Policy)

- Public

All information, whether restricted, confidential, Internal or public will be labelled accordingly, from the time it is created until the time it is destroyed or re-labelled. Such markings will appear on all manifestations of the information (hard copies, floppy disks, CD-ROMs, etc.).

This classification applies to the most sensitive business information that has limitations placed upon both its access within and disclosure outside the Oil India. Its unauthorised disclosure could seriously and adversely impact the Oil India and its stakeholders leading to legal and financial repercussions and adverse public opinion. E.g. include Merger and acquisition plans, planning for existing litigation, Board meeting notes or minutes of meeting etc.

2.2.2. Confidential

This classification applies to information that must be available for Oil India to effectively perform its mission and meet legally assigned responsibilities, and for which special precautions are taken to ensure its accuracy, relevance, timeliness, and completeness. This information, if lost, could cause significant financial loss, inconvenience, or delay in performance of the Oil India mission. E.g. include employee performance evaluations, short-term marketing plans, analyses of competitive products - services, internal audit reports, Personnel files etc.

2.2.3. Internal

This classification applies to information that is specifically meant for employees of Oil India Group. While its unauthorized discloser is against the policy, it is not expected to seriously or adversely impact the business, employees, customers, stockholders, and- or business partners. E.g. IS Policy, Acceptable Usage Policy etc.

2.2.4. Public

This classification applies to information which has been explicitly approved by Oil India management for release to the public. Public data, while subject to Oil India disclosure rules, is
available to all individuals and entities external to the Oil India community. E.g. Service brochures, advertisements, job opening announcements, and press releases

2.3. Pre-Conditions - Rules for Data Classification

• All information possessed by or used by a particular business unit within the Oil India will have a designated information owner. The information owner is responsible for assigning-maintaining appropriate data classifications.

• All files -e-mails created by individuals will be owned by them and they will be responsible for the classification of the information.

• The classification of the information will be decided by the criticality of the information and not by the media (hard copy or electronic) where the information is stored.

• All the information which is not classified will be treated as confidential.

• The classification of the media containing various classes of information will be the most critical classification of the information stored in that media.

2.4. Cumulative Classification

• The data classification levels represent cumulative information sensitivity. As the levels of sensitivity increase, the access and modification controls become more rigorous and comprehensive. For example, confidential information is a restricted subset of internal information and requires additional security controls.

2.5. Reclassification -Declassification

• The designated information owner may, at any time, change the classification of the information. To achieve this, the owner will change the classification label appearing on the original document and notify all known recipients-users.

• If known, the date that restricted or confidential information will no longer be sensitive (declassified) must be indicated on all sensitive information of the Oil India
• Date of reclassification of the information will be indicated on the classification label of the
  information.

• Information owners will periodically review the classifications of the information based on
  the sensitivity of the information.

3. Non Compliance

Failure to comply with the Data Classification Policy may, at the full discretion of the Oil India,
result in disciplinary action as per Information Technology Policy.
### Document Details

<table>
<thead>
<tr>
<th></th>
<th>Signatures with Date</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Title</strong></td>
<td>Email Usage Policy</td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>1.0</td>
</tr>
<tr>
<td><strong>Classification</strong></td>
<td>Internal</td>
</tr>
<tr>
<td><strong>Release Date</strong></td>
<td>30.05.2013</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Acceptable usage of emails by users</td>
</tr>
<tr>
<td><strong>Review Date</strong></td>
<td>30.05.2013</td>
</tr>
<tr>
<td><strong>Author</strong></td>
<td>Oil India Ltd</td>
</tr>
<tr>
<td><strong>Reviewer/Custodian</strong></td>
<td>CISO</td>
</tr>
<tr>
<td><strong>Approved By</strong></td>
<td>Information security Council (ISC)</td>
</tr>
<tr>
<td><strong>Owner</strong></td>
<td>CISO</td>
</tr>
</tbody>
</table>

### Distribution List

<table>
<thead>
<tr>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Distribution Only</td>
</tr>
</tbody>
</table>

### Version History

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Version Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Draft 0.1</td>
<td></td>
</tr>
<tr>
<td><strong>1.0</strong></td>
<td>30.05.2013</td>
</tr>
</tbody>
</table>
# Table of Content

1. Purpose .......................................................................................................................... 4  
2. Policy .......................................................................................................................... 4  
   2.1. Application ............................................................................................................. 4  
   2.2. User Responsibility .............................................................................................. 4  
   2.3. Account Creation Process ..................................................................................... 6  
   2.4. Size of Mailbox and Emails .................................................................................. 6  
   2.5. Security of Gateway PC ........................................................................................ 6  
   2.6. Management Rights to Review Email Content ..................................................... 7  
   2.7. Maintaining Email logs ....................................................................................... 7  
   2.8. Deactivation of Email Account ............................................................................ 7  
3. Non Compliance ......................................................................................................... 8
1. Purpose

This Policy supports the high level policy statements defined in Information Security Policy. Email forms a vital source of communication to carry out business processes at Oil India. The purpose of this policy is to ensure that emails are used as an efficient mode of business communication and implement control procedures so that the email services are not misused by the users. The Company should ensure that email service and operations remain secure, efficient while communicating within intranet as well as through internet.

2. Policy

2.1. Application

This policy applies to all the users of email accounts approved to be used as corporate email accounts to perform Oil India’s business communication. This includes employees, including full-time staff, part-time staff, contractors, freelancers, and other agents having email accounts in Oil India.

2.2. User Responsibility

- Users will use Company’s Email account only for the business purposes.
- Users will not use or access an Email account assigned to another employee of the organisation to either send or receive messages.
- Users will not download/forward attachments that are from an unknown or non-reliable source to prevent computer viruses.
- Users will not create or send computer viruses through Email.
- Users will zip all the attachments, where possible, while sending.
- Email client used by the users will be approved by the IT Department of the company. Use of any other client will be prohibited.
- Users will treat Email messages and files as confidential information.
- Users will not forge or try to forge email messages.
• Users will not disguise or attempt to disguise their identity while sending email messages.

• Users will not use their personal Email accounts for sending official mail. All official Email communication will take place via official Email account.

• Users will regularly archive important email messages or move these to word processing documents, text files, databases, and other files. Email systems are not intended for the archival storage of important information, as stored Email messages may be periodically purged by Systems Engineers, mistakenly erased by users, and otherwise lost when system problems occur.

• Users will not create their own, or forward externally provided Email messages which may be considered to be harassment or which may create a hostile work environment.

• In case a user encounters profane, obscure or derogatory remarks in email, he/she will either communicate with the originator of the offensive Emails, asking him/her to stop sending such messages, or report such offensive Emails directly to the respective Head and/or CISO or ISWG member.

• Users will not automatically forward their emails to any address outside the company’s networks.

• Users will not transmit/re-transmit chain messages.

• Users will request permission from their supervisor before subscribing to a newsletter or group news.

• Users will write well-structured emails and use short, descriptive subjects. The use of Internet abbreviations and characters such as smileys is not encouraged.

• User signatures will, at minimum, include employee’s name, job title and company name. Following disclaimer will be added underneath users signature:

‘The information contained herein (including attachments) is confidential and is intended solely for the addressee(s). If you have erroneously received this message, please notify the sender immediately and delete this message. If you are not the intended recipient, you are hereby notified that any disclosure, copying or distribution of this message or any accompanying document is strictly prohibited and is unlawful. Oil India Limited is not responsible for any damage caused by a virus or alteration of the e-mail by a third party or otherwise. Views or opinions in this email are not necessarily those of Oil India Limited.’
2.3. Account Creation Process

- An email account will be created for every employee joining Oil India to be used for business purposes.
- Email accounts for persons other than company employees (fulltime/part time) will be created after adequate approval from Information Security Manager.
- Email ID created will be unique and will be identified with the employee name
  
  E.g.:
  1) <first name>.<last name>@oilindia.in
  2) <first name + first letter of middle name>.<last name>@oilindia.in

2.4. Size of Mailbox and Emails

The mailbox size for each user will be restricted to a suitable size.

- The size of incoming and outgoing Emails will be restricted to 10 MB for mails received and sent outside Oil India and 5 MB for mails sent within Oil India.
- The mailbox size for the users will be restricted to the following:

<table>
<thead>
<tr>
<th>Type of user</th>
<th>Mailbox Size</th>
<th>Warning Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Senior Management</td>
<td>1 GB</td>
<td>980 MB</td>
</tr>
<tr>
<td>Other Employees</td>
<td>180 MB</td>
<td>170 MB</td>
</tr>
</tbody>
</table>

- Users will not send or receive email when the mail-box size exceeds the defined limit. The user will submit a formal request to the Systems Administrator, through the service desk tool for getting the service active.

2.5. Security of Gateway PC

- A firewall will be installed on the gateway PC, which connects the Company’s Intranet to the Internet and also handles the Remote Access connections.
• The firewall will restrict all services and ports other than minimum required for Email applications.

• Anti-virus software will to be loaded on gateway computer to detect and repair the files affected by viruses possibly coming through the Email attachments.

2.6. Management Rights to Review Email Content

• All messages sent by employees through the company Email account are company records and management reserves the right to examine them at any time and without prior notice for:
  – ensuring internal policy compliance;
  – supporting internal investigations for suspected criminal activity; and
  – assisting the management of information systems of the Company.

• Oil India reserves right to disclose Email messages sent or received through company email account to law enforcement officials without prior notice to the employees who may have sent or received such messages.

2.7. Maintaining Email logs

• The Systems Engineers will be responsible for recording, retaining, archiving and destroying Email messages and the relevant accompanying logs. The e-mail logs will be reviewed on need basis in case of suspected virus incident.

2.8. Deactivation of Email Account

• The Email ID of an employee leaving the Company will be deactivated by IT Department within 12 hrs of receiving intimation from Personnel Department. The Personnel Department will immediately notify the IT Department upon the resignation, retirement, termination or transfer of employees.

• All the emails of the employees leaving the organization will be archived before deactivating the email account only after only after approval of the reporting manager.
3. Non Compliance

Failure to comply with the E-mail Usage Policy may, at the full discretion of the Oil India, result in disciplinary action as per Information Security Policy.
How the firewall will handle applications traffic such as web, email or telnet and how the firewall will be managed and updated.
Table of Content

1. Purpose ......................................................................................................................4
2. Policy ..........................................................................................................................4
2.1 Application .................................................................................................................4
2.2 OS Hardening .............................................................................................................4
2.3 Firewall Rulebase ....................................................................................................5
2.4 Access to Firewall Platform .....................................................................................6
2.5 Firewall Policy Monitoring and Testing .................................................................7
3. Non Compliance ......................................................................................................7
1. Purpose

This Policy supports the high level policy statements defined in Information Security Policy. A firewall is a safeguard to control access between a trusted network and a less trusted network. The purpose of this policy is to define how the Company’s IT Security will be implemented using the firewall. The policy describes how the firewall will handle applications traffic such as web, email or telnet and how the firewall will be managed and updated.

2. Policy

2.1 Application

This policy document applies to all the information system assets being used at Oil India for supporting the business processes and operations at Oil India.

2.2 OS Hardening

Hardening of the host Operating System (OS) of the firewall will be carried out during installation and will be tailored to the specific operating system undergoing hardening. The following policies will be followed for OS Hardening:

- Any unused networking protocols will be removed from the firewall operating system build, as unused networking protocols can potentially be used to bypass or damage the firewall environment;
- Any unused network services or applications will be removed or disabled, as unused applications are often used to attack the firewall system;
- Any unused /unnecessary user or system accounts will be removed or disabled;
- All relevant operating system patches and hot fixes will be applied regularly. The patches and hot fixes will be tested on a non-production system prior to installation on production system;
- Unused physical network interfaces will be disabled or removed from the server chassis; and
- The practice of configuring multiple network layer (Layer 3) addresses on one physical
interface will also be avoided on firewall systems.

The above guidelines will be followed for firewalls implemented on commercial and/or open-source host OS. Some of these may not be applicable in case of an appliance firewall.

2.3 Firewall Rulebase

While assembling the firewall rulebase, the following traffic will always be blocked:

- Inbound traffic from an unauthenticated source system with a destination address of the firewall system itself. This type of packet normally represents some type of probe or attack against the firewall.

- Inbound traffic with a source address indicating that the packet originated on a network behind the firewall. This type of packet likely represents some type of spoofing attempt.

- Inbound traffic containing ICMP (Internet Control Message Protocol) traffic. Given the fact that ICMP can be used to map the networks behind certain types of firewalls, ICMP will never be passed in from the Internet, or from any untrusted external network.

- Inbound traffic from a system using a source address that falls within the address ranges set aside in RFC 1918 as being reserved for private networks. RFC 1918 reserves the following address ranges for private networks:
  - 10.0.0.0 – 10.255.255.255 (Class A)
  - 172.16.0.0 – 172.31.255.255 (Class B)
  - 192.168.0.0 – 192.168.255.255 (Class C)

Inbound traffic with these source addresses usually indicates the beginning of a denial-of-service attack.

- Inbound traffic from an unauthenticated source system containing SNMP (Simple Network Management Protocol) traffic. These packets can be an indicator that an intruder is probing a network.

- Inbound traffic containing IP Source Routing information. Source Routing is a mechanism that allows a system to specify the routes network traffic might employ while travelling from the source system to the destination system. From a security standpoint, source routing has the potential to permit an attacker to construct a network packet that bypasses firewall
controls.

- Inbound or outbound network traffic containing a source or destination address of 127.0.0.1 (localhost). Such traffic is usually some type of attack against the firewall system itself.

- Inbound or outbound network traffic containing a source or destination address of 0.0.0.0. Some operating systems interpret this address as either localhost, or as a broadcast address, and these packets can be used for attack purposes.

- Inbound traffic containing directed broadcast addresses. Directed broadcast is often used to initiate a broadcast propagation attack (such as SMURF). Directed broadcasts allow one computer system to send out a broadcast message with a source address other than its own. In other words, a system sends out a broadcast message with a spoofed source address. Any system that responds to the directed broadcast will then send its response to the system specified by the source, rather than to the source system itself. These packets can be used to create “storms” of network traffic that can used to disable websites/servers available on the Internet.

### 2.4 Access to Firewall Platform

The most common method for breaking into a firewall is to take advantage of the resources made available for the remote management of the firewall. This typically includes exploiting access to the operating system console, or access to a graphic management interface. The following will be followed for secure access to firewall platform:

- Access to the operating system console and any graphic management interface will be controlled by use of encryption and strong user authentication (at least two factor), and restricting access by IP address.

- Secure Sockets Layer will be used for graphic management interfaces that rely on the hypertext transport protocol (HTTP) for interface presentation.

- Changes to the configuration of firewalls will be done as per the change management policy.

- Procedures for backup, as prescribed by the information security policy, will be applied to back-up firewall configuration data.
2.5 Firewall Policy Monitoring and Testing

- The Firewall Administrator will audit and monitor firewall logs on a continual basis and carry out immediate actions in case of any noted exceptions.
- The Firewall Administrator will audit and verify all the firewall policies on a monthly basis. The audit report will be submitted to Information Security Manager.

3. Non Compliance

Failure to comply with the Firewall Policy may, at the full discretion of the Oil India, result in disciplinary action as per Information Security Policy.
Information Exchange Policy

Document Number: AH-IS-POL-IE-1.0

Version: 1.0
AH-IS-POL-IE-1.0 (Information Exchange Policy)

Table of Content

1. Purpose ......................................................................................................................4
2. Policy ..........................................................................................................................4
2.1 Application .................................................................................................................4
2.2 Information Exchange .............................................................................................4
3. Non Compliance .........................................................................................................6
AH-IS-POL-IE-1.0 (Information Exchange Policy)

1. Purpose

This Policy supports the high level policy statements defined in Information Security Policy. Information exchange within Company and to external parties needs to be controlled to prevent loss, modification and misuse of information. The purpose of this document is to provide directives for information exchange to be followed at the Company.

2. Policy

2.1 Application

This policy document applies to all employees, including full-time staff, part-time staff, contractors, freelancers, and other agents who have access to Oil India’s information.

2.2 Information Exchange

The following policy will be considered for Information Exchange using Company Information Systems managed by Oil India’s IT Department

- Users will be aware of the Acceptable System Usage Policy which describes responsibilities of employees and third party operational staff. Such responsibility includes but not limited to the following:
  - Data classification based information management;
  - Due precautions to be taken not to discuss confidential/restricted information in public places; and
  - Due precautions while exchanging data folders.

- Exchanged information including sensitive information contained in attachments will be protected from interception, copying, modification, misrouting, and destruction.

- Protective measure will be taken against any malicious code such as virus, worms etc. that may be transmitted due to information exchange (both inbound and outbound traffic).
AH-IS-POL-IE-1.0 (Information Exchange Policy)

- All users will protect sensitive and critical printed information by not leaving it unattended in copiers, fax machines, printers etc.

- Users will take appropriate precautions while revealing critical information on telephone to avoid being intercepted or overheard.

- Users will not leave any sensitive information on their answering machines.

- Users will be aware that fax and photocopy machines have page caches and store pages in case of a fault, which gets printed once the fault is cleared.

- Users will not register demographic data including email addresses to avoid unauthorized use.

- Owner department will consider establishing exchange agreements for Information Exchange with third parties. The following guidelines will be considered.
  
  - For any sensitive information transmitted physically, packaging should be as per defined policies;
  
  - Concerned third party will be informed about dispatch, transmission and receipt of information;
  
  - Company’s IT department will also consider entering into escrow agreements with third parties, where applicable; and
  
  - The Exchange Agreements will define responsibilities and liabilities in case of loss of information.

- Wherever possible, Company’s IT department will use only designated courier service providers for transmitting physical information.

- The Company’s IT department will consider the use of cryptographic keys/encryption technologies, where applicable.

- A labelling system will be put in place to ensure protection and appropriate handling of sensitive information.
3. Non Compliance

Failure to comply with the Information Exchange Policy may, at the full discretion of the Oil India, result in disciplinary action as per Information Security Policy.
Incident Management Policy
Document Number: OIL-IS-POL-IM-1.0
Version-1.0
Document Details

<table>
<thead>
<tr>
<th>Title</th>
<th>Incident Management Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>1.0</td>
</tr>
<tr>
<td>Classification</td>
<td>Internal</td>
</tr>
<tr>
<td>Release Date</td>
<td>01.06.2013</td>
</tr>
<tr>
<td>Description</td>
<td>Incident management requirements of Oil India</td>
</tr>
<tr>
<td>Update Date</td>
<td>01.06.2013</td>
</tr>
<tr>
<td>Author</td>
<td>CISO</td>
</tr>
<tr>
<td>Reviewer/Custodian</td>
<td>CISO</td>
</tr>
<tr>
<td>Approved By</td>
<td>Information Security Council (ISC)</td>
</tr>
<tr>
<td>Owner</td>
<td>CISO</td>
</tr>
</tbody>
</table>

Distribution List

<table>
<thead>
<tr>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Distribution Only</td>
</tr>
</tbody>
</table>

Version History

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Version Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>01.06.2013</td>
</tr>
</tbody>
</table>
Table of Content

1. Purpose ...................................................................................................................... 4
2. Policy .......................................................................................................................... 4
  2.1. Application ............................................................................................................. 4
  2.2. Reporting events and weaknesses ........................................................................ 4
  2.3. Management of incidents and improvements ....................................................... 5
    2.3.1. Responsibilities and procedures ....................................................................... 5
    2.3.2. Learning from security incidents ................................................................. 6
    2.3.3. Collection of evidence .................................................................................... 6
3. Non Compliance ......................................................................................................... 6
1. **Purpose**

This Policy supports the high level policy statements defined in Information Security Policy. ‘Incident’ refers to any event which is not part of the standard operation of a service and which causes or may cause an interruption to, or a reduction in, the quality of that service. The purpose of this policy is to ensure that untoward events associated with information, information assets, physical security and other business/IT operations are communicated and managed in a manner allowing timely corrective action to be taken. The policy establishes a consistent and effective approach to the management of incidents.

2. **Policy**

2.1. **Application**

This policy document applies to employees, including full-time staff, part-time staff, contractors, freelancers, and other agents having access to Oil India premises, assets and information including corporate data, as well as the application and systems software.

2.2. **Reporting events and weaknesses**

- IT Department will establish a formal procedure for reporting any suspected incidents (security weaknesses or threats to information systems, premises or services etc.).
- The details of the steps to be followed for reporting an incident will be communicated to all employees and third party contractors of the Company. Communication of the security incident reporting procedure will be the responsibility of the respective department.
- Users will be made aware of their responsibilities in the event of a suspected security weakness such as users will not attempt to prove (or test) a security weakness identified. Such action on part of users will be interpreted as a potential misuse of information systems and users found doing so may be liable to disciplinary action.
Users will be responsible for reporting any observed (or suspected) security weakness or any other incident immediately to the IT Department/Service Desk and will not share such information with internal or external parties.

Incident reporting and management procedure will be made available for easy access and reference for the purpose of reporting of security incidents and weaknesses by the users.

2.3. Management of incidents and improvements

2.3.1. Responsibilities and procedures

Management responsibilities and procedures will be established to ensure a quick, effective and orderly response to security incidents. The security incident management procedures will ensure that:

- Different types of incidents are clearly defined and regularly updated, e.g.
  - Information system failure and loss of service;
  - Denial of service;
  - Breaches of confidentiality and integrity;
  - Unauthorized physical access or theft;
  - Unauthorized access to the business premises;
  - Misuse of information system etc.

- Analysis and identification of the cause of the incident is undertaken;

- Guidelines are defined for categorizing the incidents based on the severity of the incidents;

- Corrective actions are defined based on the category of the incidents;

- Planning and implementation of corrective action to prevent recurrence is carried out, if necessary;

- Communication with those who are affected by or are involved in the recovery from the incident is done;

- Escalation matrix is defined based on the category of the incidents;

- Reporting the action happens to the appropriate authority;

- Audit trail and similar evidence are collected and secured; and
• All emergency actions taken are documented in detail, reported to management and reviewed in an orderly manner. The action plan will include:
  – Particulars about the business unit or department etc.;
  – Facts and explanation/reasons for the incident;
  – Severity of the incident;
  – Other business units/departments affected;
  – Corrective action to be taken;
  – Estimated cost of implementing the corrective action (if any); and
  – Estimated time frame, start date and end date.

2.3.2. Learning from security incidents

• Reported incidents will be stored and analyzed on a regular basis to determine a common action plan to prevent recurrence of such incidents.
• IT will discuss the incident records once every quarter or earlier based on the number and criticality of incidents.
• Learning from the incidents will be incorporated in Information Security Training and Awareness for the personnel.

2.3.3. Collection of evidence

• Formal procedures will be defined to ensure adequate evidence is collected for the investigations involving security incidents.
• Guidelines will be defined to assess the admissibility and weight of the evidence based on the applicable laws and published standards.

3. Non Compliance

Failure to comply with the Incident Management Policy may, at the full discretion of the Oil India, result in disciplinary action as per Information Security Policy.
Logical Access Policy
Document Number: OIL-IS-POL-LA-1.0
Version : 1.0
Document Details

<table>
<thead>
<tr>
<th></th>
<th>Signatures with Date</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Title</strong></td>
<td>Logical Access Policy</td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>1.0</td>
</tr>
<tr>
<td><strong>Classification</strong></td>
<td>Internal</td>
</tr>
<tr>
<td><strong>Release Date</strong></td>
<td>01.06.2013</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Logical access requirements of Oil India</td>
</tr>
<tr>
<td><strong>Review Date</strong></td>
<td>01.06.2013</td>
</tr>
<tr>
<td><strong>Author</strong></td>
<td>CISO</td>
</tr>
<tr>
<td><strong>Reviewer/Custodian</strong></td>
<td>CISO</td>
</tr>
<tr>
<td><strong>Approved By</strong></td>
<td>Information Security Council (ISC)</td>
</tr>
<tr>
<td><strong>Owner</strong></td>
<td>CISO</td>
</tr>
</tbody>
</table>

Distribution List

<table>
<thead>
<tr>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Distribution Only</td>
</tr>
</tbody>
</table>

Version History

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Version Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>01.06.2013</td>
</tr>
</tbody>
</table>
Table of Contents

1. **Purpose** ...................................................................................................................... 4
2. **Policy** .......................................................................................................................... 4
2.1. **Application** ............................................................................................................. 4
2.2. **User Identification and Creation** ........................................................................... 4
2.3. **Control of User ID** ............................................................................................... 5
2.4. **User Transfer or Termination Controls** ................................................................. 6
2.5. **Network Access** ...................................................................................................... 6
   2.5.1. Policy on use of network services ................................................................. 6
   2.5.2. User authentication for external connections ................................................ 6
   2.5.3. Network device access controls .................................................................... 7
   2.5.4. Network device authentication and security ................................................ 7
   2.5.5. Wireless network security .............................................................................. 8
   2.5.6. Remote diagnostic and configuration port protection .................................... 8
   2.5.7. Segregation in networks .................................................................................... 8
   2.5.8. Network connection control ............................................................................ 8
   2.5.9. Network routing control .................................................................................... 9
3. **Non Compliance** ......................................................................................................... 9
1. Purpose

This Policy supports the high level policy statements defined in Information Security Policy. The purpose of this policy is to establish systems and procedures for user account management, privilege management and network access management in order to protect and safeguard information and information assets at Oil India from unauthorized access and to ensure the confidentiality, availability and integrity of the information and information assets. The policy will help in managing new account, transfer and removal of account and privileged account management based on the business needs at Oil India.

2. Policy

2.1. Application

This policy document applies to all employees, including full-time staff, part-time staff, contractors, freelancers, and other agents who have access to Oil India’s information and/or information assets.

2.2. User Identification and Creation

- User account for new employees will be created by IT on the request of concerned department head. Intimation mail will be sent to all the stakeholders on creation of new account. Additional application level access will be provided after formal authorization from the line manager and application owner.

- In case of contractors/agents, requests for creation of user account is raised by the Manager and approved by the supervisor and respective application owner.

- There will be a formal user access creation and deletion procedure for granting access to all multi-user information systems and services.

- All users will be granted access to computing resources through unique user identification (UID). The UID will be created using employee’s name.
OIL-IS-POL-LA-1.0 (Logical Access Policy)

- User authorization credentials will consist of a User ID and password. Records for the user IDs will be maintained by the IT Department with full name, job title and contact information. A Log register will be maintained by each section of IT department for record.

- IT Department will provide the password information to process head for first time login in. The user will change the password on first time login as per the Password Management Policy.

- Standard domain privileges will be provided to the user based on his/her roles and responsibilities identified. Any exception to the same will be approved by the Functional Manager and Information Security Manager for the business.

- Use of common user IDs or group user IDs will not be allowed. Any exception to the same must be approved by the Functional Manager and the Information Security Manager. The same must be reviewed on a quarterly basis.

2.3. Control of User ID

- IT Department will perform the user access review at least once in three months.

- Default user IDs shipped with software and hardware will be disabled immediately. Alternatively, the passwords will be changed in accordance with the Password Management Policy.

- The use of the Guest user ID or any other generic user ID is prohibited. Specific user IDs will be created to facilitate individual tracking/accountability.

- Five unsuccessful attempts lock the account. A root cause is then to find the cause of lock out.

- Screensaver password will be used and screensaver will get activated after 5 minutes of inactivity.

- Computer clocks will be set accurately to ensure accuracy of audit logs. The System Engineers in charge of the network will ensure that users cannot change the settings.

- User activities will be logged on the system depending upon the criticality and business requirements. The logs will be reviewed by the respective Systems Engineers and
investigated upon in case of any unusual activity. Procedures will be defined to carry out corrective actions immediately.

2.4. User Transfer or Termination Controls

- The Human Resource Department will immediately notify the IT Department upon the resignation, termination or transfer of employees. IT Department will deactivate all the UIDs upon termination or resignation of employees and revoke or modify access upon transfer of responsibilities within 72 hrs of receiving notification from HR.
- All user IDs deactivated will be deleted after 30 days of deactivation unless otherwise requested by the concerned user department.

2.5. Network Access

2.5.1. Policy on use of network services

- Users will only have direct access to the services that they have been specifically authorized to use.
- Users will not establish any external network connections that could permit third party users to gain access to Company systems and information, unless prior approval from IT Department has been obtained.
- When using Company information systems, or when conducting Company business, users will not deliberately conceal or misrepresent their network identity.

2.5.2. User authentication for external connections

- Users will be provided remote access for the basic functionalities as per business requirements through SSL Gateway. The use of any additional remote access will be authorised by the Functional Manager and IT Department.
- All users remotely accessing the Company computer and networks will ensure that they are authenticated with passwords through SSL gateway.
- Inbound connection to Company computers or networks through an office desktop modem will be prohibited unless specific approval has been obtained from the IT Department.
OIL-IS-POL-LA-1.0 (Logical Access Policy)

- Outbound connection to third-party networks including the Internet through office desktop modems or other types of modems will be approved by the IT Department.

- Leaving personal computer-linked modems in auto-answer mode will be prohibited unless a remote user identification system approved by the IT Department is being used.

2.5.3. Network device access controls

The IT team will document the access rules / tables for network gateways including routers and firewalls. In addition, to the rules on the firewall, the permitted services in the network will also be documented.

The network access controls to be configured on the firewall or switches will be decided based on the business needs of Oil India. Every router will meet the following configuration standards:

- Disallow the following:
  - IP directed broadcasts, unreachable & redirects;
  - Incoming packets at the router sourced with invalid addresses such as RFC1918 address (in gateway devices connected to internet);
  - TCP small services;
  - UDP small services;
  - All source routing;
  - All web services running on device;
  - Proxy ARP; and
  - Use corporate standardized SNMP community strings which should not be default.

2.5.4. Network device authentication and security

The following control will be implemented to ensure a secure identification and authentication process for network devices:

- Remote access will be permitted only for authorized users. As per policy by default all laptop users are authorized users.
OIL-IS-POL-LA-1.0 (Logical Access Policy)

- Access or any change in the access levels will require authorization from the Functional Manager and Information Security Manager.
- The network communication of any user connecting to the network remotely will be terminated on providing three consecutive incorrect passwords.
- Confidential information will be encrypted before being transmitted over a remote access connection.
- Remote Access logs will be generated and maintained in CISCO Network Management System.
- Remote users will be automatically disconnected from the Oil India network after predefined session time irrespective of the inactivity. The user must then login again to reconnect to the network.

2.5.5. Wireless network security
- Access to the wireless network will be password protected as per the Password management Policy.
- All wireless LAN access will use corporate-approved vendor products and security configurations.

2.5.6. Remote diagnostic and configuration port protection
- Access to all diagnostic ports will be provided after approval from CISO. Connection to the remote diagnostic ports will be provided using secure communication channels.

2.5.7. Segregation in networks
- All “walk-up” network access for visitors to connect back to their home networks will employ a separate subnet that will not have any connection to the Company internal network.

2.5.8. Network connection control
- All Company internal network devices will have common passwords as per the asset class and changed once in a quarter. Unattended active internal network ports that connect to the Company internal computer network will not be placed in public areas including, but not limited to, building lobbies, company cafeterias, and conference rooms, unless segregated
OIL-IS-POL-LA-1.0 (Logical Access Policy)

from the Company internal computer network.

- All network ports in common areas that are not routinely in use will be promptly disconnected at the wiring closet or at another centralized location.

2.5.9. Network routing control
- All Company internal networks will be divided into security zones wherever appropriate.
- All Company internal networks will have routing controls to ensure that computer connections and information flows do not breach the access control policy of the business applications.

3. Non Compliance

Failure to comply with the Logical Access Security Policy may, at the full discretion of the Oil India, result in disciplinary action as per Information Security Policy.
OIL-IS-POL-LC-1.0 (Legal Compliance Policy)

Document Détails

<table>
<thead>
<tr>
<th></th>
<th>Signatures with Date</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Title</strong></td>
<td>Legal Compliance Policy</td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>Version 1.0</td>
</tr>
<tr>
<td><strong>Classification</strong></td>
<td>Internal</td>
</tr>
<tr>
<td><strong>Release Date</strong></td>
<td>03.06.2013</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Applicable legal, regulatory and contractual requirements of Oil India</td>
</tr>
<tr>
<td><strong>Review Date</strong></td>
<td>03.06.2013</td>
</tr>
<tr>
<td><strong>Author</strong></td>
<td>Oil India Ltd</td>
</tr>
<tr>
<td><strong>Reviewer/Custodian</strong></td>
<td>CISO</td>
</tr>
<tr>
<td><strong>Approved By</strong></td>
<td>Information security Council (ISC)</td>
</tr>
<tr>
<td><strong>Owner</strong></td>
<td>IT Department, OIL</td>
</tr>
</tbody>
</table>

Distribution List

<table>
<thead>
<tr>
<th>Name</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Internal Distribution Only</td>
</tr>
</tbody>
</table>

Version History

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Version Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Draft 0.1</td>
<td></td>
</tr>
<tr>
<td><strong>1.0</strong></td>
<td>03.06.2013</td>
</tr>
</tbody>
</table>
Table of Contents

1.  Purpose .......................................................................................................................... 4
2.  Policy ........................................................................................................................... 4
   2.1.  Identification of Applicable Legislation ............................................................... 4
   2.2.  Intellectual Property Rights .................................................................................. 5
   2.3.  Software Compliance ......................................................................................... 5
3.  Non Compliance ........................................................................................................... 6
1. Purpose

This Policy supports the high level policy statements defined in Information Security Policy. The purpose of this policy is to clearly illustrate that Oil India intends to fully comply with the applicable legal, regulatory and contractual requirements that affect the organization’s activities.

2. Policy

2.1. Identification of Applicable Legislation

- Oil India will identify and comply with all the applicable statutory, regulatory, legal and contractual obligations.
- The following legislations shall be applicable to Oil India:
  - IT Act : Quarterly compliance requirements
  - Income Tax Act 1961 : Quarterly compliance requirements
  - Labour Laws : Quarterly compliance requirements
  - Central/ State Sales Tax Act : Quarterly compliance requirements
  - Companies Act 1956 : Quarterly compliance requirements
  - Employees Profession Tax : Quarterly compliance requirements
  - Service Tax Act : Quarterly compliance requirements
  - Customs Act : Quarterly compliance requirements
  - Copyright Act : Quarterly compliance requirements
  - Trade Marks Act : Quarterly compliance requirements
  - Indian Contract Act : Quarterly compliance requirements
OIL-IS-POL-LC-1.0 (Legal Compliance Policy)

- Payment of Gratuity Act: Quarterly compliance requirements
- EPF & Miscellaneous Act, 1952: Quarterly compliance requirements
- Employee Pension Scheme, 1995: Quarterly compliance requirements

- All employees/third party users and contractors will be made aware of the applicability of these legislations by the Legal Department.
- All statutory and contractual obligations identified by the company will be reviewed at least once a year for adherence and applicability. The results will be used to update all relevant policies and procedures as applicable.
- Statutory audits will be performed by internal and external teams as applicable to measure the compliance with applicable legislation.
- The Information Security Working Group will ensure compliance with all applicable legislation with coordination from Finance department.

2.2. Intellectual Property Rights

- All the copyrighted information of Oil India will be used only for business purposes. (Ex: Company logo)
- Strict action will be taken against those who misuse Oil India copyrighted material as per the Disciplinary Process. Examples of misuse include unauthorized transmission of copyrighted material outside Oil India, utilizing copyrighted material for personal use etc.

2.3. Software Compliance

- All software used within Oil India will be purchased and issued in accordance with the license agreements. Oil India will take strong disciplinary action against any person engaging in unauthorized copying of licensed software.
- No shareware (beyond its period of free use), or pirated software must be used on Oil India’s computer equipment.
Approval will be taken from the IT head for use of shareware and freeware on Oil India computer resources.

The use or copying of purchased software on a computer other than the computer for which it is licensed is strictly prohibited.

IT head will ensure that maximum number of users permitted for usage of software does not exceed the number of licenses.

The Information Security Working Group and IT team will conduct periodic reviews to detect and discourage unauthorized software being used. All illegal software found during such reviews will be removed or uninstalled immediately by the IT team.

3. Non Compliance

Failure to comply with the Legal Compliance Policy may, at the full discretion of the Oil India, result in disciplinary action as per Information Security Policy.
Laptop & Desktop Security Policy

Document Number: OIL-IS-POL-LDS-1.0

Version: 1.0
Physical and logical security of Laptop and desktops
Table of Contents

1. Purpose ...........................................................................................................................................4
2. Policy ................................................................................................................................................4
   2.1 Application ....................................................................................................................................4
   2.2 Users’ Responsibilities..................................................................................................................4
   2.3 Laptop and Desktop Inventory Management .................................................................................4
   2.4 Return of Laptop ...........................................................................................................................4
   2.5 Physical Security ..........................................................................................................................5
   2.6 Logical Security ...........................................................................................................................5
   2.7 Maintenance ................................................................................................................................6
       2.7.1 Hardware Maintenance ...........................................................................................................6
       2.7.2 Software Maintenance ...........................................................................................................6
3  Non Compliance ..............................................................................................................................7
1. Purpose

This Policy supports the high level policy statements defined in Information Security Policy. The policy ensures that physical and logical security of Laptop and desktops and the security of the data residing on them will be maintained. They will be protected against damage, loss or unauthorized access.

2. Policy

2.1 Application

This policy applies to all the employees, including full-time staff, part-time staff, contractors, freelancers, and other agents having access to Laptop or desktop that belongs to Oil India or contains Information that belongs to Oil India. This Policy does not Include Laptops under Executive Laptop Scheme.

2.2 Users’ Responsibilities

Users will be responsible for protection of Laptop and Desktop being used by them and will ensure it is secure in their absence. Laptop and Desktop will be issued, maintained and returned as per relevant policy and applicable regulations.

2.3 Laptop and Desktop Inventory Management

- All Laptops and desktops will have & be labeled with an Asset Number. This Asset Number will be flexible and scalable for future organization growth.

  All allotment of Laptop and desktops will be via an Asset Allocation Form only and recorded in the asset register appropriately

2.4 Return of Laptop

- The Asset Coordinator will instruct the asset manager/ administrative staff to collect the Laptop from the user leaving the organization or getting transferred.
The asset manager/ administrative staff will check for the physical damage of the device.

The asset manager/ administrative staff will take the signature from the user on the Electronic Asset Allocation form after receiving the device.

### 2.5 Physical Security

- All Desktops will be located in secure areas to protect from physical damage and unauthorized access.
- Laptops will be kept in locked offices/cabinets when not in use.
- Laptop custodians will ensure physical safety of such asset in public places (like airports, hotels, conferences, etc.).
- Any add-on hardware components connected to the Laptop will be protected from theft and damage.
- When staying in hotels, users will lock their laptops in cupboards when they are not in. If room security is not of a high order, then users must take it with them.
- On flights, laptops will be carried as hand/cabin baggage.
- Users are advised to take extra precautions when in crowded areas like bus/train stations, airports, parks etc.
- If user's Laptop is stolen, users will immediately notify the police or security as well as IT department/ administration department, and give them specific information to identify the device.
- Users must also keep their Laptop make, model, and serial number in some other place that is separate from their device or device bag.

### 2.6 Logical Security

- The initial configuration of the laptop and desktops will:
  - Install only minimal required software for operation of the respective user group;
**OIL-IS-POL-LDS-1.0 (Laptop & Desktop Security Policy)**

- Remove all unnecessary system utilities;
- Keep BIOS write password confidential; and
- Install anti-virus software with latest updated signatures and engine versions.

- Any additional application software will be installed on laptops and desktops only after proper approval from the IT department.
- The installation, up-gradation and de-installation of software on laptops and desktops will be done by identified personnel only.
- Users will take adequate precautions to protect sensitive data on their systems. They should back up the data in the system regularly.
- Users are prohibited from storing any unauthorized software or pornographic content on to the Oil India network.
- All laptops and desktops will display wallpapers and screen savers pre-approved and standardized by Oil India. The screensaver will be automatically activated after 5 min. of inactivity.
- Users will lock their laptops and desktops while leaving their desks.
- Power on passwords shall be used to prevent unauthorized booting of the desktops.
- Local Administrator user name will be renamed.
- Users are strictly prohibited from tampering with or attempting to modify the Registry on Windows based systems.

### 2.7 Maintenance

#### 2.7.1 Hardware Maintenance
- Laptop and desktops will be under AMC.

#### 2.7.2 Software Maintenance
- Laptop and desktops will be constantly updated with patches for the operating system and all the applications.
3 Non Compliance

Failure to comply with the laptop & Desktop Security Policy may, at the full discretion of the Oil India, result in disciplinary action as per Information Security Policy.
Media Management Policy
Document Number: OIL-IS-POL-MM-Version 1.0
Version 1.0
Document Details

<table>
<thead>
<tr>
<th>Title</th>
<th>Media Management Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Version 1.0</td>
</tr>
<tr>
<td>Classification</td>
<td>Internal</td>
</tr>
<tr>
<td>Release Date</td>
<td>01.06.2013</td>
</tr>
<tr>
<td>Description</td>
<td>Stipulates controls to prevent unauthorized disclosure, modification, removal or destruction of information residing on storage media</td>
</tr>
<tr>
<td>Review Date</td>
<td>01.06.2013</td>
</tr>
<tr>
<td>Author</td>
<td>CISO</td>
</tr>
<tr>
<td>Reviewer-Custodian</td>
<td>CISO</td>
</tr>
<tr>
<td>Approved By</td>
<td>Information Security Council (ISC)</td>
</tr>
<tr>
<td>Owner</td>
<td>CISO</td>
</tr>
</tbody>
</table>

Distribution List

Name

Internal distribution only

Version History

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Version Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 1.0</td>
<td>01.06.2013</td>
</tr>
</tbody>
</table>
Table of Contents

1. Purpose ......................................................................................................................4
2. Policy ..........................................................................................................................4
  2.1 Application ...........................................................................................................4
  2.2 Users’ Responsibilities ........................................................................................4
  2.3 Management of Removable Media ....................................................................4
  2.4 Disposal of Media ..............................................................................................5
  2.5 Information Handling ........................................................................................6
  2.6 Security of system documentation ...................................................................6
3. Non Compliance ......................................................................................................7
1. Purpose

This Policy for Media Management supports the high level policy statements defined in Information Security Policy. All media containing sensitive information will be protected. This policy intends to protect the company’s sensitive Information by preventing unauthorized disclosure, modification, removal or destruction of information assets that may lead to interruptions to business activities. This will also minimize the risk of sensitive information leakage to unauthorized persons.

2. Policy

2.1 Application

This policy document applies to all Oil India employees, its contractors, its associates and other individuals affiliated with Third Parties who have access to Oil India information resources which includes computers whether server or client, all network equipment, infrastructure equipment, operating systems, messaging systems, software, output devices and storage mediums.

2.2 Users’ Responsibilities

Users will be responsible for protection of Removable Media being used by them and will ensure its storage in lock and key in their absence. Removable computer media will be recycled/disposed off as per relevant policy and applicable regulations.

2.3 Management of Removable Media

Procedures will be defined for the management of removable computer media, such as tapes, disks, cassettes, USB drives and printed reports, ensuring:

- Sensitive information will not be stored with non-sensitive information on any removable storage media. Electronic information, belonging to the Oil India, will be stored in accordance to the Information Exchange policy.

- If no longer required, the previous contents of any re-usable media that are to be removed from the organization will be erased and made un-recoverable.
Authorization will be required for all media removed from the organization and a record of all such removals to maintain an audit trail will be kept.

All media will be stored in a safe and secure environment and in accordance with the manufacture’s specifications.

Information stored on media that needs to be available longer than the media lifetime (in accordance with manufacturers’ specifications) will also be stored elsewhere to avoid information loss due to media deterioration.

All data stored on removable media will be evaluated against the Company’s Asset Valuation and Classification Guideline and protected in the manner outlined in the Media Management Policy.

Removable media like USB drives to be disabled/controlled if possible.

### 2.4 Disposal of Media

Procedures will be defined for the secure and safe disposal of Media when no longer required, ensuring:

- Media containing information valued as sensitive will be physically destroyed when required for use any more.

- Records of disposal, including time of destruction, name of person who destroyed it and means of disposal will be maintained.

- When accumulating media for disposal, consideration will be given to the aggregation effect, which may cause a large quantity of unclassified information to become more sensitive than a small quantity of classified information.

- Procedures will be defined to identify items that might require secure disposal.

- In cases where contractors are used for collection and disposal services for paper, equipment and media, care will be taken while selecting a suitable contractor with sufficient experience and which complies with the Information Security Policy.
Secret information will be immediately destroyed when due for destruction and confidential information that is to be destroyed will be placed in a designated locked destruction container within Company’s offices and will never be placed in trash bins, recycle bins, or other publicly-accessible locations.

2.5 Information Handling

Procedures for the handling and storage of information will be established in order to protect information from unauthorized disclosure or misuse, ensuring:

- All media will be labelled and handled as per the classification level in which the media is classified.
- Sensitive information will not be removed from the Company’s premises unless there has been prior approval from the Information Owner and must be logged with a record of the date, the information involved, and the persons possessing the information.
- Upon creation, all data will be saved to a network drive. If data is incomplete or is only for individual use, it may be stored on the local drive.
- Any data created while not connected to the network will be copied to the network upon reconnection and then removed from the local drive if no longer required.

2.6 Security of system documentation

- Prior to being released to third parties, all documentation that describes Oil India’s information systems or systems procedures will be reviewed by IT Department. This review will be recorded to maintain an audit trail.
- All the system documentation will be stored in an environment secured as required by the Company’s Information Security Policy.
- Access list for system documentation will be kept to a minimum and authorized by the application owner.
- Procedures will be defined to protect system documentation held on a public network, or supplied via a public network.
3. Non Compliance

Failure to comply with the Media Management Policy may, at the full discretion of the Oil India, result in disciplinary action as per Information Security Policy.
Program Development Policy
Document Number: OIL-IS-POL-PD-1.0
Version : 1.0
**Document Details**

<table>
<thead>
<tr>
<th></th>
<th>Signatures with Date</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Title</strong></td>
<td>Program Development Policy</td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>1.0</td>
</tr>
<tr>
<td><strong>Classification</strong></td>
<td>Internal</td>
</tr>
<tr>
<td><strong>Release Date</strong></td>
<td>01.06.2013</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Establish controls around program development and provide a framework for security controls</td>
</tr>
<tr>
<td><strong>Review Date</strong></td>
<td>01.06.2013</td>
</tr>
<tr>
<td><strong>Author</strong></td>
<td>CISO</td>
</tr>
<tr>
<td><strong>Reviewer/Custodian</strong></td>
<td>CISO</td>
</tr>
<tr>
<td><strong>Approved By</strong></td>
<td>Information Security Council (ISC)</td>
</tr>
<tr>
<td><strong>Owner</strong></td>
<td>CISO</td>
</tr>
</tbody>
</table>

**Distribution List**

<table>
<thead>
<tr>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Distribution Only</td>
</tr>
</tbody>
</table>

**Version History**

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Version Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>01.06.2013</td>
</tr>
</tbody>
</table>
# Table of Content

1. Purpose .......................................................................................................................... 4
2. Policy ............................................................................................................................. 4
2.1 Application ................................................................................................................... 4
2.2 Program Development ............................................................................................... 4
   2.2.1 Requirement gathering/analysis ........................................................................... 4
   2.2.2 Planning and Design ............................................................................................. 5
   2.2.3 Development ......................................................................................................... 6
   2.2.4 Development Testing .......................................................................................... 6
   2.2.5 Release .................................................................................................................. 7
3. Non Compliance ............................................................................................................ 8
1. Purpose

This Policy supports the high level policy statements defined in Information Security Policy for Oil India. Oil India’s application development team carries out program development to meet in-house needs. To ensure uniformity, software quality/functionality, better performance and security, Oil India application development team needs to follow a set of standard guidelines and procedures. The purpose of this policy is to establish controls around program development and provide a framework for security controls that have an impact on risks relating to the development environment such as operational errors, technical failures, software malfunction etc.

2. Policy

2.1 Application

This policy document applies to all program developments carried at Oil India by employees of application development team (both full-time and part-time) and/or third party.

2.2 Program Development

Software development framework at Oil India for program development can be mapped to the following phases:

2.2.1 Requirement gathering/analysis

- The business requirements for the program development will be captured in the Requirement Form prepared by the Application Owner. The concept note will be approved by the CIO and forwarded to the IT Head.
- The program development team will be responsible for analysing the concept note and understanding and gathering the IT/security requirements for the development. The information security requirements will be addressed and fulfilled in accordance with the organization’s information security policies and procedures.
A business functionality requirement assessment will be performed to understand the possible changes and the changes required in the standard operating procedures of the business operation(s) getting impacted.

A security/risk assessment will be performed in the development phase to determine levels (i.e., low, moderate, or high) of potential impact on the organization’s information system assets which may lead to a security breach/policy violation resulting in loss of confidentiality, integrity, or availability of information assets.

Based on the risks identified, suitable security requirements will be documented and addressed by the program development team.

System/application/database security features will be detailed as much as possible: these will include but are not limited to form of authentication, required level of encryption, authorization mechanisms/parameters, logging/audit trail, and system deployment considerations.

2.2.2 Planning and Design

The analysis of the security and business functionality performed in the requirements gathering phase will be adequately addressed in the solution design. The security and operational features required will be analyzed for feasibility and method of implementation.

Adequate planning will be done to ensure that the agreed upon security and business controls are fully documented. The security plan will also provide a complete description of the information system as well as any other references such as key documents supporting the information security program (e.g., change and configuration management, risk assessment, security test and evaluation results, system interconnection, security authorizations, deployment scenarios etc.).

Also, business controls and operational controls will be adequately defined and documented to ensure compliance with company business and operational policies e.g. payment, content management, payroll etc. These controls then will be reviewed and approved by the respective business owner.
A project manager will be identified who will be responsible for the managing the entire project through all its phases. A detailed project plan detailing activities and timelines, responsible personnel, etc., will be prepared by the Project Manager.

### 2.2.3 Development

- Application development team will address source code control by ensuring adequate versioning. The application developer/s will perform code related activities on their respective workstations and the source code will be versioned accordingly.
- Coding standards and guidelines will be defined and documented and the program development will be carried out by the program development team in accordance with these coding standards and guidelines.
- Where there is a requirement to use third party tools/software (e.g. open source) for development purposes, the Information Security Manager will be consulted prior to its use. This will ensure that Oil India is safeguarded against Intellectual property right violations. Existing software are reviewed once and if new versions are rolled out it is reviewed again.
- It will be ensured that the necessary security requirements are addressed in the initial phase of the development.
- Where requirements arise relating to feature enhancements and bug fixing, the Change Management Procedure will be followed and relevant documentation will be maintained.
- The development environment for the application development must be separated from the production environment along with the respective teams.

### 2.2.4 Development Testing

- To ensure that software developed by application development team is defect free and meets the quality standards and requirements of the customer (both internal and external) it is crucial that software testing be performed by an independent testing team and the business user/s other than the developers of the application.
- The QA and testing environment for performing the testing of the application developed will be separate from the production environments along with the respective teams.
- The tests to be performed will be carried out in a separate environment that is segregated (logically or physically) from the production environments. Access to these environments
will be controlled by the IT Infrastructure team and only restricted to the authorized users. The following will be addressed as part of development/security features testing:
- The security features required have been developed as per the functionality; and
- The security features developed are effective and cannot be circumvented.

• Test data (cases and results) will be documented and maintained separately from the live data.

• Cases for User Acceptance Testing (UAT), functional testing, integration testing, system testing will be developed and their results documented and maintained.

• Input Data Validation - The input data for the application systems will be validated before saving/committing a transaction.

• The following checks will be considered when entering data fields:
  - Out-of-range values (e.g. negative values, extremely large or small inputs etc.);
  - Invalid characters;
  - Data in the compulsory fields;
  - Duplicate values in key fields;
  - Error messages generated in the event of incorrect input data; and
  - Recovery/rollback plans for incorrect input data.

• Wherever possible, procedures will be built into the programs to correct or propose corrections to the input data if certain errors are detected by the system.

• Control of Internal Processing - The programs will be designed to ensure accurate internal processing. Design of such system will incorporate different validation checks to identify processing errors. E.g. buffer overruns, hash totals of records / files, programs are invoked in the right processing order etc.

• Output Data Validation - The application systems will validate the data being generated from the application system after processing of the stored information to ensure that the data is correct and appropriate. E.g. control counts to check validity of output data.

### 2.2.5 Release

• The following individuals will be involved in the phase post development testing:
  - Quality manager
Implementation team*
- IT Infrastructure personnel *

- The Quality manager will check for coding standards, completeness of development and testing (i.e. all required system and security functionalities have been developed and tested). This can be checked by viewing records of documentation at various stages of the Program Development and code reviews. Checks for the following will be carried out:
  - Change management processes have been followed;
  - All required sign-offs have been obtained at various stages of the Application Development; and
  - Formally acknowledgement/sign-off on the release/implementation of the software product.

- On completion of the above requirements, the IT Infrastructure team member/s will migrate the released version of the application to the production environment.

* - If required

3. Non Compliance

Failure to comply with the Program Development Policy may, at the full discretion of the Oil India, result in disciplinary action as per Information Security Policy.
### Document Details

<table>
<thead>
<tr>
<th></th>
<th>Signatures with Date</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Title</strong></td>
<td>Physical and Environmental Security Policy</td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>Draft 0.1</td>
</tr>
<tr>
<td><strong>Classification</strong></td>
<td>Internal</td>
</tr>
<tr>
<td><strong>Release Date</strong></td>
<td>01.06.2013</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Physical and Environmental Security controls of Oil India</td>
</tr>
<tr>
<td><strong>Review Date</strong></td>
<td>01.06.2013</td>
</tr>
<tr>
<td><strong>Author</strong></td>
<td>CISO</td>
</tr>
<tr>
<td><strong>Reviewer/Custodian</strong></td>
<td>CISO</td>
</tr>
<tr>
<td><strong>Approved By</strong></td>
<td>Information Security Council (ISC)</td>
</tr>
<tr>
<td><strong>Owner</strong></td>
<td>CISO</td>
</tr>
</tbody>
</table>

### Distribution List

<table>
<thead>
<tr>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Distribution Only</td>
</tr>
</tbody>
</table>

### Version History

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Version Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>01.06.2013</td>
</tr>
</tbody>
</table>
**Table of Content**

1. **Purpose** ........................................................................................................................... 4
2. **Policy** ............................................................................................................................. 4
   - 2.1. **Application** ......................................................................................................... 4
   - 2.2. **Secure Areas** .................................................................................................... 4
   - 2.3. **Equipment Security** ........................................................................................ 9
3. **Non Compliance** ............................................................................................................. 12
1. Purpose

This Policy supports the high level policy statements defined in Information Security Policy. Information Assets are required to be physically protected from security threats to prevent loss, damage or compromise assets which may lead to disruption of business continuity. Physical & Environmental Security refers to the protection of office site and equipment (and all other information and information assets) from theft, vandalism, natural disaster, manmade catastrophes, and accidental damage (e.g., from electrical surges, extreme temperatures etc.) which may lead to disruption of business operations. The purpose of this document is to describe the acceptable and non acceptable activities to prevent unauthorized access, damage and interference of business premises and information.

2. Policy

2.1 Application

The policy applies to employees, including full-time staff, part-time staff, contractors, freelancers, and other agents accessing Oil India business premises and information assets.

2.2 Secure Areas

2.2.1 Physical Security Perimeter

Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) will be used to protect areas that contain information and information processing facilities. Physical protection will be achieved by creating several physical barriers around the business premises and information processing facilities. Each barrier establishes a security perimeter, creating a defence in depth strategy and eliminating a single point of failure.

The following guidelines and controls will be considered and implemented where appropriate:

- The security perimeter will be clearly defined;
The perimeter of a building or site containing information processing facilities will be physically sound (i.e. there will be no gaps in the perimeter or areas where a break-in could easily occur). The external walls of the site will be of solid construction and all external doors will be suitably protected against unauthorized access, e.g. control mechanisms, alarms, locks etc;

- A manned reception area or other means to control physical access to the site or building will be in place. Access to Oil India premise is restricted to authorized personnel only;
- Physical barriers will, if necessary, be extended from real floor to real ceiling to prevent unauthorized entry and environmental contamination such as that caused by fire and flooding; and
- All fire doors/exits on a security perimeter will be access controlled, monitored, and tested in conjunction with the walls to establish the required level of resistance.

2.2.2 Physical Entry Controls

Secure areas will be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. The following controls will be implemented to ensure adequate protective measures:

- Each employee will be issued proximity card for entry to secure areas along with an identification card which will have the following details:
  - Employee name
  - Unique Employee ID
  - Photograph
  - Business Unit
  - Blood Group + emergency contact numbers
- Department Employees who have forgotten their identification badge/proximity card will obtain a temporary badge after approval team leader. This will not have access to floors such a temporary badge will stay valid for a single day only. The employee needs to return the temporary badge while leaving the office.
• Identification badges that have been lost or stolen or are suspected of being lost will be reported instantly. Such cards will be deactivated once mail is received from the employee or any other user with immediate effect.

• All temporary workers, trainees, consultants, engineers who require access to secure areas will be issued a temporary card after approval from their respective SPOC and immediate superior in the Department. This will not have access to floors. Such a temporary badge will stay valid for a single day only. The employee needs to return the temporary badge while leaving the office.

• Visitors to secure areas will be supervised, and their date and time of entry along with the photo identity proof and departure recorded.

• All personnel will be required to wear their identification card at all times and will be encouraged to challenge unescorted strangers and anyone not wearing visible identification.

• Access rights to secure areas will be regularly reviewed on quarterly basis and updated by management responsible for the specified areas.

2.2.3. Securing offices, rooms and facilities
A secure area may be a locked office or several rooms inside a physical security perimeter, which may be locked and may contain lockable cabinets or safes. The selection and design of a secure area will take into account the possibility of damage from fire, flood, explosion, accident, malicious intent, and other forms of natural or man-made disaster. Consideration will be given also to any security threats presented by neighbouring premises, e.g., leakage of water from other areas.

The following controls are essential considerations:

• Key facilities will be sited to avoid public access;

• Buildings will be unobtrusive and will give minimum indication of their purpose;

• Doors and windows will be locked when unattended and external protection will be considered for windows, particularly at ground level;
• Hazardous or combustible materials will be stored securely at a safe distance from a secure area. Bulk supplies such as stationery will not be stored within a secure area until required.

• Fallback equipment and back-up media will be sited at a safe distance to avoid damage from a disaster at the main site.

• Any outlying buildings or areas that house/contain data centre support equipment (backup generators, UPS, etc) will have the similar level of security controls as the data centre itself; secure structure, access control, and technical surveillance systems for monitoring access and activities around the area. CCTV may be implemented to track movement at all critical entry and exit points. The recordings of CCTV will be kept for next 15 days. Surveillance and monitoring is subject to legal limitations in many jurisdictions, and will be subject to contractual limitations in union, Works Council or shop agreements. Legal Counsel will be consulted before implementing these measures.

• A manned reception area or other means to control physical access to the building will be in place. Access to the building will be restricted to authorized-personnel only.

• Visitor and Escort Control procedures will be implemented to ensure that all visitors to the company facilities are positively identified and authorized prior to granting access. Visitors to secure areas will be escorted or cleared for unescorted access, and their date and time of entry and departure recorded. Visitors will only be granted access for specific, authorized purposes. Visitor photo pass logs will be established and maintained. Wherever possible, Technical Surveillance Systems (CCTV) will be utilized to monitor activities around the immediate environs of the building and entrances.

• All safety/fire emergency doors will be access controlled and have closing and locking mechanisms along with hooters in case if it is opened.

• Special care will be given to ensure the security of loading areas.

2.2.4 Working in Secure Areas

The following guidelines may be considered:
Access to sensitive information and information processing facilities, will be controlled and restricted to authorized persons only. Authentication controls, (e.g. Card/Badge Access Control System), will be used to authorize and validate all access. An audit trail of all access will be securely maintained. These secure areas will also include telephone and network closets, environmental, UPS and server room etc.

All personnel will be required to wear identification badges, and security personnel may challenge unescorted strangers and anyone not wearing visible identification.

Access rights to secure areas will be regularly reviewed (quarterly) and updated;

Personnel will only be aware of the existence and activities in a secure area on a need to know basis;

Unsupervised working in secure areas will be avoided both for safety reasons and to prevent opportunities for malicious activities; and

Vacant secure areas will be physically locked and periodically checked.

2.2.5 Isolated Delivery Loading Areas

Delivery and loading areas will be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

The following controls will be considered:

Access to a holding area from outside of the building will be restricted to identified and authorized personnel;

The holding area will be designed so that supplies can be unloaded without delivery staff gaining access to other parts of the building;

Incoming material will be inspected for potential hazards and registered, if appropriate, before it is moved from the holding area to the point of use; and

Incoming and outgoing shipments will be physically segregated; wherever required.
2.3  Equipment Security

2.3.1  Equipment Location and Protection
LAN servers, routers, midranges, mainframe, PBX’s and other computer hardware which would not typically reside on an individual user’s desktop or in common working areas will be physically located in a secured area, with adequate controls for preventing or suppressing environmental hazards like fire and other non-environmental threats such as theft which could hamper availability of data.

The following guidelines will be considered for protecting the equipments:

- Equipment will be located to minimize unnecessary access into work areas;

- Information processing facilities handling sensitive data will be positioned and the viewing angle restricted to reduce the risk of information being viewed by unauthorized persons during their use, and storage facilities secured to avoid unauthorized access;

- Items requiring special protection will be isolated to reduce the general level of protection required;

- Controls will be adopted to minimize the risk of potential physical threats, e.g. theft, fire, explosives, smoke, water (or water supply failure), dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation, and vandalism;

- Smoke detectors and fire extinguishers/ water sprinklers may be placed at all strategic locations across Oil India premises to set off an alarm in case of fire; and

- Random checks/rounds will be carried to ensure that eating, and smoking in proximity to information processing facilities is not carried out.

2.3.2  Power Supplies
Computer hardware will be protected from electrical problems that might cause a computer malfunction or failure. Magnets or sources of magnetic fields will not be located near computer diskettes or tapes. Examples include radios, magnetic picture and/or coat hangers, flashlight magnets, magnetized screwdrivers, paper clip holders, transformers and motors.
The following options for continuity of power supplies will be used:

- Multiple feeds to avoid a single point of failure in the power supply;
- Uninterruptible power supplies (UPS); and
- Back-up generator.

2.3.3 Cabling Security

Power and telecommunications cabling carrying data or supporting information services will be protected from interception or damage.

The following controls will be considered:

- Power and telecommunications lines into information processing facilities will be underground, where possible, or subject to adequate alternative protection;
- Network cabling will be protected from unauthorized interception or damage. Examples of this protection include using conduit or avoiding routes through public areas; and
- Network distribution areas will be physically secured to prevent unauthorized access or modification.
- For sensitive or critical systems armoured conduit and locked rooms or boxes will be installed at inspection and termination points.

2.3.4 Equipment Maintenance

Equipments will be correctly maintained to ensure their continued availability and integrity.

The following controls will be considered:


**2.3.5 Security of Equipment off-premises**

Security will be applied to off-site equipment taking into account the different risks of working outside the organization’s premises.

The following controls will be considered:

- Equipment and media taken off the premises will not be left unattended in public places;
- Manufacturers’ instructions for protecting equipment will be observed at all times, e.g. protection against exposure to strong electromagnetic fields; and
- Adequate insurance cover will be in place to protect equipment off-site.

**2.3.6 Secure disposal or re-use of equipment**

All items of equipment containing storage media will be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal. Devices containing sensitive information will be physically destroyed or the information will be destroyed, deleted or overwritten using techniques to make the original information non-retrievable rather than using the standard delete or format function.

**2.3.7 Removal of Property**

Equipment, information or software will not be taken off-site without prior authorization.

The following controls may be considered:

- Equipment, information or software will not be taken off-site without prior authorization;
• Employees, contractors and third party users who have authority to permit off-site removal of assets will be clearly identified;

• Equipment will be recorded as being removed off-site and recorded when returned; and

• A log of items, facilities and keys in possession of employees will be maintained.

3 Non Compliance

Failure to comply with the Physical & Environmental Security Policy may, at the full discretion of the Oil India, result in disciplinary action as per Information Security Policy.
Document Details

<table>
<thead>
<tr>
<th></th>
<th>Signatures with Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Password Management Policy</td>
</tr>
<tr>
<td>Version</td>
<td>Version 1.0</td>
</tr>
<tr>
<td>Classification</td>
<td>Internal</td>
</tr>
<tr>
<td>Release Date</td>
<td>01.06.2013</td>
</tr>
<tr>
<td>Description</td>
<td>Acceptable usage of password management by users</td>
</tr>
<tr>
<td>Review Date</td>
<td>01.06.2013</td>
</tr>
<tr>
<td>Author</td>
<td>CISO</td>
</tr>
<tr>
<td>Reviewer-Custodian</td>
<td>CISO</td>
</tr>
<tr>
<td>Approved By</td>
<td>Information Security Council (ISC)</td>
</tr>
<tr>
<td>Owner</td>
<td>CISO</td>
</tr>
</tbody>
</table>

Distribution List

<table>
<thead>
<tr>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Distribution Only</td>
</tr>
</tbody>
</table>

Version History

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Version Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 1.0</td>
<td>01.06.2013</td>
</tr>
</tbody>
</table>
# Table of Content

1. Purpose ...................................................................................................................... 4  
2. Policy .......................................................................................................................... 4  
   2.1. Application ................................................................................................................. 4  
   2.2. User Responsibility ................................................................................................. 4  
   2.3. Confidentiality of Passwords ...................................................................................... 5  
   2.4. Password Composition ............................................................................................... 5  
   2.5. One time use of initial password: ............................................................................... 6  
   2.6. Password reset ........................................................................................................... 6  
   2.7. Super User Password ............................................................................................... 6  
   2.8. Power on passwords ................................................................................................. 7  
   2.9. Disabling default passwords .................................................................................... 7  
   2.10. Confidentiality of Password ................................................................................ 7  
   2.11. Password Management ...................................................................................... 7  
3. Non Compliance ......................................................................................................... 8
1. Purpose

This Policy supports the high level policy statements defined in Information Security Policy. Access to user accounts is controlled by an authentication mechanism utilizing unique user IDs and passwords. These authentication mechanisms ensure controlled and restricted access to the information and information systems according to the business requirements. The purpose of this policy is to establish the rules for the creation, distribution, safeguarding, termination, and reclamation of the user authentication mechanisms.

2. Policy

2.1. Application

This policy document applies to all employees, including full-time staff, part-time staff, contractors, freelancers, and other agents who have access to Oil India’s Network and/or information.

2.2. User Responsibility

- Each user will have a unique user identification code and password to access Company’s Computer systems.
- Users will be personally responsible and accountable for all actions performed under their user account.
- Users will be responsible for protecting their user accounts, passwords and other access codes entrusted to them.
- Users will ensure that:
  - after accessing Computer Systems the machines are logged off;
  - machine is not in use prior to logging on to a computer system;
  - passwords are not written down and stored anywhere around the work place; and
  - passwords are not shared with any person for any reason (not even with administrators).
OIL-IS-POL-PM-Version 1.0 (Password Management Policy)

- Users will not use the same password for Oil India accounts as for other non Oil India accounts.
- Users will not share their passwords with anyone through any mode of communication like phone, email, questionnaires-security forms etc.
- "Remember Password" feature is not be used for any applications.
- In case an account or password is suspected to have been compromised, users will
  - Report immediately to the IT Department; and
  - Reset passwords suspected to have been compromised immediately.

2.3. Confidentiality of Passwords

- All Users (normal users, administrators) passwords will remain confidential and will not be shared posted or otherwise divulged in any manner. Passwords will not be stored in clear text on computer systems and will be stored in an encrypted format. Also, passwords will not be displayed on system reports.

2.4. Password Composition

- The password will be at least 8 characters long
- Users will change password at least once in 45 days
- Last five password will not be used again
- User will not use user name as password
- Password will meet at least three conditions among below four
  - Password will contain Lower case characters
  - Password will contain Upper case characters
  - Password will contain Numerical
  - Password will contain Special characters
- Five unsuccessful attempts lock the account. A root cause should be done to find the cause of lock out.
OIL-IS-POL-PM-Version 1.0 (Password Management Policy)

- Users will not use easy to guess passwords such as company name, names of pets, spouse, favorites, vendor supplied default passwords, etc.
- Password will not be a word in any language, slang, dialect, jargon, etc. or based on personal information, names of family, phone number etc.

2.5. One time use of initial password:
- An initial non-standard temporary password will be provided to the users & communicated securely to the reporting leaders by the IT Department. The system will be configured to force the users to change the initial password immediately after the first logon.
- In application systems, where this functionality of force changing the password is not available, the user will change the password manually. Information system owners will be responsible for making the users of such application system aware of the need for manually changing the passwords on first logon.

2.6. Password reset
- User will request for reset of password to the IT Helpdesk. The department will verify the identity of the user by verifying the employee number and then reset the password. The new password will be a one-time password and will be changed immediately when reset by the system administrator.

2.7. Super User Password
- All privileged user passwords for Operating Systems, Databases, Applications, Network Equipment like routers, switches etc., will be sealed in an envelope and kept in a fire proof safe. This is necessary in case the password is forgotten or the related person has left the organization without surrendering the passwords.
- These sealed envelopes will be opened with the permission of the CISO. The password will be changed immediately and kept in a new sealed envelope. Details of such activity will be logged appropriately. All privileged user passwords will be changed once in 90 days.
2.8. Power on passwords

- Users will be required to use the power-on passwords (for critical workstations and laptops), which will be sealed, in an envelope in fire proof safe. Sharing of power-on passwords will be allowed only if multiple users need to access the same system physically and the passwords will be maintained solely within the members of the group sharing the system. Such sharing will be allowed only after approval from the CISO.

2.9. Disabling default passwords

- Vendor Supplied User-IDs/Passwords, encryption keys, and other access codes included with vendor-supplied systems will be changed before a new system is brought on-line. Similarly, default passwords shipped with software will be disabled or changed before the software is deployed in the production environment.

2.10. Confidentiality of Password

- All User (normal users, administrators) passwords will remain confidential and not shared, posted or otherwise divulged in any manner.
- Passwords will not be stored in clear text on computer systems and will be stored in an encrypted format.
- Passwords will not be displayed on system reports.
- Display and printing of passwords will be masked, suppressed, or otherwise obscured.
- Passwords will be conveyed to users in a secure manner. Passwords will never be disclosed via telephone or through third parties or through unprotected (clear text) electronic mail messages.

2.11. Password Management

- Password Reset: will be carried out only by the Service Desk on request from the users. The team will verify the employee number of the user before executing the request for password change. The users will be asked to change their passwords immediately.
- Users will be provided with the capability to change their password on the login interface.
OIL-IS-POL-PM-Version 1.0 (Password Management Policy)

- **Screen Saver Password**: All workstations, laptops and servers will have a screen saver password which will come up within 5 minutes of inactivity.

- All passwords will be immediately changed if they are suspected of being disclosed, or known to have been disclosed to unauthorized parties.

3. **Non Compliance**

Failure to comply with the Password Management Policy may, at the full discretion of the Oil India, result in disciplinary action as per Information Security Policy.
**Document Details**

<table>
<thead>
<tr>
<th></th>
<th>Signatures with Date</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Title</strong></td>
<td>Physical Security Manual</td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>1.0</td>
</tr>
<tr>
<td><strong>Classification</strong></td>
<td>Internal</td>
</tr>
<tr>
<td><strong>Release Date</strong></td>
<td>01.06.2013</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Manual describing the physical security for OIL Premises</td>
</tr>
<tr>
<td><strong>Review Date</strong></td>
<td>01.06.2013</td>
</tr>
<tr>
<td><strong>Author</strong></td>
<td>CISO</td>
</tr>
<tr>
<td><strong>Reviewer/Custodian</strong></td>
<td>CISO</td>
</tr>
<tr>
<td><strong>Approved By</strong></td>
<td>Information Security Council (ISC)</td>
</tr>
<tr>
<td><strong>Owner</strong></td>
<td>CISO</td>
</tr>
</tbody>
</table>

**Distribution List**

<table>
<thead>
<tr>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Distribution Only</td>
</tr>
</tbody>
</table>

**Version History**

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Version Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Draft 0.1</td>
<td></td>
</tr>
<tr>
<td><strong>1.0</strong></td>
<td>01.06.2013</td>
</tr>
</tbody>
</table>
Table of Contents

1. Purpose ......................................................................................................................4
2. Introduction................................................................................................................4
3. Key Practice Details....................................................................................................4
4. Miscellaneous procedures for Physical security.......................................................12
1. Purpose

This document provides the physical security manual for OIL.

2. Introduction

This document refers to the controls implemented by the organization in order to maintain physical security of the premises with special emphasis to following areas:

- Zoning of premises.
- Physical security
  - CCTV
  - Access Control
- Environmental threats

3. Key Practice Details

o Zoning of Physical Premises

2.1.1 Premise for zoning and types of zones

The need of segregating OIL premises into various categories arises from the need for adequate controls in the non-public area.

The premises have been marked into four areas:

a. Public
b. Internal
c. Restricted
• **Public Areas**

The following form part of the public area:

• Reception Area;
• Meeting Rooms near reception area;
• Washrooms near reception area; and
• Fire Exits.

All visitors, candidates for interviews and any other third party visiting organization’s premises are required to record their details in a visitor entry register kept at the manned reception area. All such parties should be issued a visitor card by the facilities after which they are escorted to their respective destinations.

Access to public areas is given to all employees, visitors, guests, third parties etc.

• **Internal Areas**

The following form part of the restricted areas:

• Work Area;
• Meeting Rooms/ Conference Rooms in Work Areas;
• Pantry Area; and
• Photocopier Area

Access to internal areas is guarded by security guards and a visitor entry register is maintained for entry of any personnel other than the dedicated staff.

Access to restricted areas is given to Employees and third party staff (as authorised).

• **Restricted Area**

The following form part of critical areas:

• Server room;
• UPS room.

Access to Server Room is restricted and is provided only to people working in the IT team and other employees & third party staff (as authorised).
OIL-IS-POL-PSM-1.0 (Physical Security Manual)

Access to UPS room is restricted to the IT Team only. Entry of personnel other than designated is to be recorded in the register maintained for the purpose near the UPS room. After working hours; keys are kept with the security guard for emergency purposes.

2.1.2 Procedure for Zoning
IT Department is responsible for zoning of premises. On the ‘diagram’ of the site various areas are to be defined by the IT Department and properly marked. These diagrams are to be signed by the IT Head and kept in custody of the IT Head for any future reference. There shall not be more than two copies of such diagram (s); one with IT Head and one in fire proof safe for safe keep.

The zoning is done by appropriately segregating the premises in to Public Area, Internal Area and Restricted Area. The segregation is done by:

- Specific Marking on Floor Plan;
- Physical Marking in premises (optional);
- Implementing the Access Controls/restrictions;
- Modifying the nature of Equipments, Supporting Utilities & their arrangement; and
- Installing specific accessories (if required).

2.1.3 Process for review and revision of zoning
The zoning diagram is to be reviewed and updated by IT Head in consultation with the security team once every financial year or as and when redesigning of area takes place. The old diagram will be replaced by the new diagram and filed appropriately.

Physical Security Measures

2.1.4 Specification of Physical Security Measures
OIL may implement following security measures in the premises to prevent any unauthorised entry to premise and safeguarding of assets.
OIL-IS-POL-PSM-1.0 (Physical Security Manual)

- CCTV cameras may be installed;
- Access control mechanism to recognise authorised access; and
- Manned reception area and entry/exit points.
  - Security against Environmental threats

2.1.5 Identification of Environment Threat (Natural and Man Made)
The following environmental hazards have been identified by the management and Information Security Working Group (ISWG):

- Fire
- Flood
- Earthquake
- Explosion
- Lightning
- Civil Unrest
- Humidity

2.1.6 Mitigation measures for environmental threat(s)

- **Fire**
  - OIL may install smoke detectors, water sprinklers and fire extinguishers in the premises.
  - Fire Exits have been clearly demarcated and the Fire Exit Plans have been displayed on all floors.
  - Fire alarm and fire fighting system comprising of smoke detectors, sprinkler system and portable extinguishers have been installed.

- **Flood**
  - Contacts have been established with various authorities to seek help in case of eventualities.

- **Civil Unrest**
  - Contacts have been established with various authorities to seek help in case of eventualities.
Earthquake
Contacts have been established with various authorities to seek help in case of eventualities.

Explosion
Contacts have been established with various authorities to seek help in case of eventualities.

Lightning
Suitable lightning arrestors have been installed.

Humidity
Air Conditioners have been installed in server room. All supporting utilities including Air conditioners are regularly maintained to ensure proper functioning.

Safeguarding Physical Security Equipment

2.1.7 CCTV Camera Equipment
CCTV Camera equipment may be installed and monitored round the clock.

Guidelines for working in restricted areas

2.1.8 Access to Restricted Areas
Access to restricted area is accorded only to authorised employees and third party staff. Following guidelines are observed for working in restricted areas:

- Inflammable materials such as matchboxes, lighters, gas are not allowed inside the restricted areas.
- All refuse (paper or wooden boards, packing materials, etc.) should be immediately removed from the restricted area after the work is over.
- Any activity under the raised floor which can damage the cables, fire detectors wires, and other sub floor devices and equipment must be carried out under expert supervision or IT manager’s supervision.
- Eatables and drinks are not allowed inside the restricted areas.
- Mobile phones which may interfere with the functioning of the instruments are not allowed inside the restricted areas.
Physical Access Management

2.1.9 Authorization process for access to internal areas

- **Employees**
  A person who is on the employee rolls of OIL and is bound by the rules and regulations of OIL is an OIL employee.

- All OIL employees are issued photo ID cards to be displayed while being at OIL premises.

- Access Card issued to all employees will be used to gain access to control areas within the building. This access card is personal to an individual and hence shall not be shared with co-workers.

- It is responsibility of every employee to challenge anyone not displaying an ID card or, a temporary pass and ask for proof of their identity. Those persons failing to prove their identity shall be escorted to Security / Reception desk, where appropriate action shall be taken.

- In case an employee does not bring his identity & access card on any particular day, he/she will be issued a temporary card with an access to work area with a validity of one day only. The card will only be issued if the employee is identified by his/her project manager/team member in the physical access register kept at the main gate. The temporary card will have to be surrendered by the employee at the time of leaving the office premises on the same day. Admin will maintain a log of all temporary access cards along with the record of the person who identified the employee. The reconciliation of all issued temporary cards will be carried out at the end of day to prevent any misuse.

- **Visitors**
  Visitors are defined as persons who are not OIL employees. Agency temporary staff and contractors who have not been issued with a personal ID card must be treated as visitors for the purpose of granting access to OIL premises.

- Only visitors (including ex-members of staff) who have a legitimate business reason and have been previously notified to site Security will be permitted to enter Company premises. Visitors who require access beyond public areas will be issued with a visitor badge.
• All visitors need to enter their contact details viz. name, company, purpose of visit, contact number, address, time and date of entry and name of visited person in the visitor entry register.

• Visitors will also be required to declare IT assets including laptops, hard discs, CDs, pen drives etc in the visitor entry register at the time of entry.

• Visitors will be issued a visitor card for easy identification, after being identified by an employee of OIL. While in office premises, visitors need to be escorted at all times by an employee or a security guard.

• **Third Parties**
Any person who is not an employee of OIL and requires access to the information systems under contractual engagement.

• Access requests for third party personnel shall be routed by the onsite manager of the third party for approval. The remaining procedure for authorization and granting/removing access shall be the same as that for OIL employees. Post authorization, third parties will be issued identification badges and access cards with minimal rights as may be required to perform their job. If access is required for less than a week, the third party personnel may be treated as visitors.

• Third Party personnel will be issued an access cards card for easy identification.

• For the interim period when the access card has not been obtained but applied for, the third party personnel shall be treated as visitors and will have to follow the same procedure that is applicable to visitors accessing the premises.

### 2.1.10 Identity Badges

• All employees will be required to display their Identity badge at all times when in the company premises. Neckbands for all employees will bear ‘OIL’ for easy identification.

• Visitors may be issued a visitor card with a visitor neckband bearing ‘Visitor’ for easy identification, after being identified by an employee of OIL. While in office premises, visitors need to be escorted at all times by an employee or a security guard.
• Third party staff will be issued a vendor card with a neckband bearing ‘Vendor’ for easy identification.

2.1.11 Lost Identification Badges / Access Cards
In the event of an access card being missing, employees/ third parties and visitors are required to report to the security immediately. The admin team will in turn be required to de-activate the missing access card. In the event that an unattended access card is found, it is to be returned to the admin team and they are required to deactivate it immediately.

2.1.12 Access to dedicated and critical areas

• Employees:
Employees requiring access to restricted areas as identified above, will require authorisation from the manager of the area, before admin team grants access. The access of an employee should not exceed the access provided to his reporting manager.

• Visitors:
Visitor entering restricted areas like server room, UPS rooms, BMS room etc. will have to record their details viz. name, company, purpose of visit, contact number, address, time and date of entry and employee escort in access registers maintained for these areas and will be supervised at all times by the escort.

• Third party staff:
Third party staff working onsite will be granted access as identified above. Third party personnel who require temporary access to critical and dedicated areas will be treated as visitors.

2.1.13 Surrender of Access Card

• Employees:
Admin is informed of termination/ separation of employees by Personnel Department. Separating employees are required to surrender the access card to Admin on their last day in the company. On surrender of access card the employee will be escorted out of the work area by the admin manager/ security guard. Access for all terminated employees is removed as soon as intimation is received from Personnel Department of the same.
A register will be maintained with the admin team, which records the details of the access card returned before it is reissued to a new user.

**Visitors:**
All visitors need to return the identification badges issued to them while leaving OIL premises. The security guard on duty needs to ensure return of all cards issued on a particular day.

**Third Parties:**
In the event of the third parties leaving/ resignation/ termination of contract, the vendor onsite manager shall send communication to admin team. The personnel will surrender the access card to their onsite manager from the vendor end, who will submit the same to security. These cards will be deactivated immediately.

### 2.1.14 Monitoring and Review of Access Rights
There will be regular monitoring of access rights of all employees and third parties having access by OIL Cards. This will be undertaken by the Admin team at least once in six months and reported to Admin head for review. This review will be carried out on various parameters like whether access rights of terminated/ separated employees have been removed, temporary access cards issued and not received back, access rights of third party staff etc.

### 4. Miscellaneous procedures for Physical security

- **Physical locking of the premises**

#### 2.1.15 When will the premises be physically locked
The door has to be locked only if there is no employee working inside the premises. The premises (or part of premises) remain locked over the weekend or holiday if there is no employee present in the premises. The premises may, however, be opened by the security personnel for regular housekeeping activities.

#### 2.1.16 Responsibility of keys and recording of data
The guard on duty will carry the keys to the physical lock present on the door, and would only handover the keys to the next guard on the duty. The monitoring of this exchange of keys will be recorded in the security guard handover register.
2.1.17 Locking of Office Cabins
There are certain cabins in OIL that have been allocated to key personnel. Such cabins are to be physically locked by the concerned key person at the time of leaving for the day. These cabins are opened only at the instruction (can be a standing instruction such as to open the cabin in the morning every day) of the person concerned and regular housekeeping activities need to be supervised by a security guard.

2.1.18 Keys to Cupboards, Lockers etc
Keys to all lockers are kept in custody of the respective employees. Group specific cupboards are marked and identifiable. Unmarked cupboards do not contain any restricted or confidential information. It is the responsibility of the manager of the team allotted the cupboard to safe keep the keys. In case of a need for a lost key, the respective manager will request the Admin Head, who will arrange for the duplicate key, and will hand it over to the Manager.

Fire Safety Processes

2.1.19 Checking of Fire Extinguishers
Labelling or checking for manual fire extinguishers for refill dates and checking of effective pressure will be done on a periodic basis.

2.1.20 Checking of fire sprinklers and fire detection System
Periodical check-up of fire sprinklers, fire alarm system will be done and logs will be maintained in the equipment maintenance register.

2.1.21 Fire Drill

- Fire drills will be carried out in conjunction with building officials.
- Admin Head will inform the employees through email, and Fire Marshals will guide the employees about the fire safety and evacuation procedures.
- Proper signage of fire exits and emergency exit plan to be installed at appropriate places for effective evacuation.
- Fire Drill to be carried out on half yearly basis to keep employees updated on the evacuation procedures.
Mailroom Security

All packets, envelopes, cartons etc. will be opened at the rear gate security room. A dedicated security agent duly authorized will open all packets, envelops, cartons etc and check the internal contents. This person will again staple /paste / seal those packets and will emboss an OK Security Check stamp on each and every packet and hand over these mails / courier packs to internal mail room agents. A dedicated courier entry register will be maintained for the same.
Removable of Property Policy

Document Number: OIL-IS- POL-RP –Version 1.0

Version 1.0

Oil India Limited

(A Government of India Enterprise)
Description
Policy stipulates the confidentiality and availability of the information and restricts unauthorized movement or removal of information assets.

Review Date
01.06.2013

Author
CISO

Reviewer/Custodian
CISO

Approved By
Information Security Council (ISC)

Owner
CISO

Version History

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Version Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 1.0</td>
<td>01.06.2013</td>
</tr>
</tbody>
</table>

Distribution List

Name
Internal Distribution Only
# Table of Content

1. **Purpose** ................................................................................................................................. 4
2. **Policy** ....................................................................................................................................... 4
   2.1 Application ............................................................................................................................. 4
   2.2 Users’ Responsibilities ........................................................................................................... 4
   2.3 Authorization .......................................................................................................................... 4
   2.4 Recording & Monitoring ....................................................................................................... 5
3. **Non Compliance** ..................................................................................................................... 5
1 Purpose

This Policy supports the high level policy statements defined in Information Security Policy. The movement of Information Assets from a location to another location or a removal of an Information Asset must be authorized and recorded. The purpose of this policy is to restrict unauthorized movement or removal of Information Assets and ensure the confidentiality, integrity and availability of the information.

2 Policy

2.1 Application

This policy applies to all employees, including full-time staff, part-time staff, contractors, freelancers, and other agents having access to information assets at Oil India.

2.2 Users’ Responsibilities

Users must ensure that any movement or removal of an Information Asset must be authorized and recorded. Users must also be responsible for reporting any unauthorized movement or removal of an Information Asset, if identified.

2.3 Authorization

- Formal procedure, standards or guidelines for movement of property will be implemented. The Head of Security department, or a representative, will be responsible for the implementation and maintenance of the same.
- Information processing equipment, information, storage media or software will not be taken off-site without prior authorization from the asset owners or departmental managers.
- Users who have authority to permit off-site removal of assets will be clearly identified.
- All computer storage media leaving Oil India offices will be accompanied by a properly authorized pass and will be logged at designated entry/exit points.
**Oil-IS-POL-RP-Version 1.0 (Removable of Property Policy)**

### 2.4 Recording & Monitoring

- Gate-passes will clearly indicate if the asset is non-returnable. For all other types of assets, time limits for removal will be indicated and returns checked for compliance.
- Equipments will be recorded as being removed off-site and recorded when returned.
- Random spot checks will be performed to detect unauthorized removal of information assets and unauthorized information assets into the site.

### 3 Non Compliance

Failure to comply with the Removal of Property Policy may, at the full discretion of the Oil India, result in disciplinary action as per Information Security Policy.
Technical Vulnerability and Patch Management Policy

Document Number: OIL-IS-POL-TVPM-1.0

Version : 1.0
To ensure a consistent approach is applied to the management of technical vulnerabilities and all available patches.

Review Date: 30.05.2013

Author: CISO

Reviewer/Custodian: CISO

Approved By: Information Security Group

Owner: CISO

---

### Version History

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Version Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Draft 0.1</td>
<td></td>
</tr>
<tr>
<td>1.0</td>
<td>30.05.2013</td>
</tr>
</tbody>
</table>
# Table of Content

1. Purpose ...................................................................................................................... 4
2. Policy .......................................................................................................................... 4
   2.1. Application ............................................................................................................. 4
   2.2. Vulnerability Risk Assessment and Management ........................................... 4
   2.3. Patch Management .......................................................................................... 5
3. Non Compliance ......................................................................................................... 6
1. Purpose

This Policy supports the high level policy statements defined in Information Security Policy. The policy stipulates that the technical vulnerabilities in IT department’s information systems are identified and addressed in a timely manner. The policy also ensures that a consistent approach is applied to the management of technical vulnerabilities and that all available patches of the software used by the Company’s IT department are assessed, approved, implemented and reviewed in a control manner. This would also ensure that all software patches applied on the information systems are in accordance with the approved business and technical requirements.

2. Policy

2.1. Application

This policy document applies to all employees, including full-time staff, part-time staff, contractors, freelancers, and other agents of IT Department and who have access to Oil India information system and or Network.

2.2. Vulnerability Risk Assessment and Management

- The Chief Information Security Officer (CISO) will ensure that periodic risk assessments are conducted as per the Information Security Manual.

- The implementation of procedures for asset management and tracking will be the responsibility of the Chief Information Security Officer (CISO);

- The IT Head will designate IT personnel for identifying technical vulnerabilities on Company information systems. Additionally, designated personnel from IT will proactively stay in touch with vendors/ specialist groups to keep abreast with latest resources;

- On identification of a potential technical vulnerability the following actions will be taken:
  - The vulnerability identified will be communicated to all the relevant personnel in the IT department;
  - Any risks associated with it will be identified; and
Appropriate measures will be taken, after internal approval to patch these vulnerabilities to mitigate any risks associated with it.

- The IT Head will ensure that the vulnerability assessment is performed and the weaknesses identified are resolved as per the defined periodicity.

- Vulnerability assessment will be performed semi-annually preferably by internal team.

- If any patches are available to mitigate identified vulnerabilities, the patches will be tested, logged and evaluated in a separate test environment before they are installed on Company’s computer systems.

- If no patches are available to address the vulnerabilities, then one or more of the following actions will be taken:
  - Stopping the services related to vulnerabilities;
  - Creating or modifying access control rules on Firewall, Proxy Server and other such servers; and
  - Create awareness among the users and personnel, involved in maintenance of the computer system, about technical vulnerabilities.

### 2.3. Patch Management

- The Company’s IT Department will document and implement a Patch Management Process including enhancements and resolution procedures. This will be applicable for patches available for software installed on the department’s information processing facilities.

- Procedures will be defined and responsibility designated to identify new security issues related to information processing facilities and any new patches released by the vendor.

- All new patches will be prioritized based on factors such as nature of the patch, vendor criticality, risk to the un-patched system in current environment and any other applicable parameter.

- A formal process for prioritization of patches and implementation schedule will be defined.

- Patches that require the information processing facility to be taken off-line will not be applied during business hours. In case of emergency patches, the IT Head and the
information asset owner will approve implementation during the working hours after adequate communication to all the stakeholders and the IT users getting impacted.

- Patches will be tested in a test environment prior to application in production systems. Results of the tests conducted will be submitted to the asset owner/IT Head who will approve or decline the changes required.

- Quarterly reviews will be done to assess if the Company’s IT department information systems are patched with the latest appropriate patches. Such reviews will also take inputs from technical vulnerability assessments conducted previously (Refer: Section 2.2).

- The IT Head will be responsible for implementing the procedures required to conduct the above-stated reviews and addressing any gaps identified.

3. Non Compliance

Failure to comply with the Technical Vulnerability and Patch Management Policy may, at the full discretion of the Oil India, result in disciplinary action as per Information Security Policy.
## Document Détails

<table>
<thead>
<tr>
<th></th>
<th>Signatures with Date</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Title</strong></td>
<td>Audit Logging and Monitoring Procedures</td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>1.0</td>
</tr>
<tr>
<td><strong>Classification</strong></td>
<td>Internal</td>
</tr>
<tr>
<td><strong>Release Date</strong></td>
<td>01.06.2013</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Procedure for Audit Logging and Monitoring</td>
</tr>
<tr>
<td><strong>Review Date</strong></td>
<td>01.06.2013</td>
</tr>
<tr>
<td><strong>Author</strong></td>
<td>CISO</td>
</tr>
<tr>
<td><strong>Reviewer/Custodian</strong></td>
<td>CISO</td>
</tr>
<tr>
<td><strong>Approved By</strong></td>
<td>Information Security Council (ISC)</td>
</tr>
<tr>
<td><strong>Owner</strong></td>
<td>CISO</td>
</tr>
</tbody>
</table>

## Distribution List

<table>
<thead>
<tr>
<th>Name</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Distribution Only</td>
<td></td>
</tr>
</tbody>
</table>

## Version History

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Version Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Draft 0.1</td>
<td></td>
</tr>
<tr>
<td><strong>1.0</strong></td>
<td>01.06.2013</td>
</tr>
</tbody>
</table>
# Table of Contents

1. Audit Logging and Monitoring .......................................................... 4
2. Audit trail rules ................................................................................. 4
3. Monitoring system use ..................................................................... 4
   3.1. Monitoring of firewall logs ......................................................... 5
   3.2. Use of Intrusion detection system ............................................. 5
4. Deployment of a central syslog server ............................................. 6
5. Security Audits ................................................................................. 6
1. Audit Logging and Monitoring

All computing resources not limited to server, desktops, laptops, network devices should be monitored to ensure conformity to logical access policies and procedures. This is necessary to determine the effectiveness of measures adopted and to ensure conformity to logical access policies and procedures.

2. Audit trail rules

Audit trails recording exceptions and other security-related events should be logged for all computing resources available within the OIL network not limited to user and admin accounts. The logs generated would be kept for a quarter to assist in future investigations and access control monitoring. All logs stored should be protected from unauthorized access. All logs should be in “Read only” format and un-editable even by the system administrator. A record of successful system access, in addition to rejected attempts, should be created. At a minimum, audit trails must include the following:

- User ID’s
- Dates and times for logon and logoff
- Terminal identity or location if possible

All logs would be reviewed periodically by the Network/System Administrator and report submitted to IT Head.

3. Monitoring system use

The systems use must be monitored to ensure that users are only performing processes that have been explicitly authorized. The level of monitoring required for individual systems should be determined by a separate risk assessment. Areas that must be monitored are:

- Access failures
- Review of logon patterns for indications of abnormal use or revived user IDs


**OIL-IS-PRO-ALM-1.0 (Audit Logging and Monitoring Procedures)**

- Allocation and use of user accounts including users with admin rights
- Tracking of selected transactions
- The use of sensitive resources
- Dial-up activity
- Firewall activity
- O/S and application access attempts

**3.1. Monitoring of firewall logs**

The Systems Engineers must review the Internet connection audit reports created on the firewall for any unusual/suspicious activities. The period between reviews should not exceed two days. This shall be a part of the daily activities performed by the system engineer and will be recorded in the Daily Checklist. Alarms must be configured to alert the Systems Engineers of Systems Operations Group about any suspected activities, security breaches or violations and any other related events generated by the firewall. The events to be monitored include, but not limited to:

- A session being initiated from the external world
- Spoofing activities
- Suspicious activities taking place internally and from external sources
- A new server/host attaching to the network locally and remotely
- Well known hacker signatures
- Password guessing attempts
- Attempts to use privileges that have not been authorized
- Modification to system software.

**3.2. Use of Intrusion detection system**

- Network Intrusion Detection Systems (NIDS) should be deployed to monitor network traffic to and from the network segments hosting sensitive information resources viz. critical applications.

- Host based Intrusion Detection Systems (HIDS) should be considered for deployment on critical or high value information assets/systems.
The intrusion detection systems should be configured to send critical alerts to the concerned system and security administrators on a real-time basis. Further, the IDS logs should be reviewed and documented on a weekly basis by the concerned system and security administrators.

4. Deployment of a central Syslog server

A centralized logging server (viz. syslog server) should be deployed for gathering logs from various systems, firewalls and IDS in a centralized location. Log analysis tools should be used for analyzing the logs collected in the logging server. The capacity of the syslog server should be planned accordingly.

5. Security Audits

Internal security compliance audits not limited to Software compliance audit, Network security audit, internal audits shall be conducted on an annual basis.
Procedure for Control of Documents

Document Number: OIL-IS-PRO-COD-1.0

Version : 1.0
### Document Details

<table>
<thead>
<tr>
<th>Title</th>
<th>Procedure for Control of Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>1.0</td>
</tr>
<tr>
<td>Classification</td>
<td>Internal</td>
</tr>
<tr>
<td>Release Date</td>
<td>30.05.2013</td>
</tr>
<tr>
<td>Description</td>
<td>Procedure for control of Oil India documents</td>
</tr>
<tr>
<td>Review Date</td>
<td>30.05.2013</td>
</tr>
<tr>
<td>Author</td>
<td>CISO</td>
</tr>
<tr>
<td>Reviewer/Custodian</td>
<td>CISO</td>
</tr>
<tr>
<td>Approved By</td>
<td>Information Security Council (ISC)</td>
</tr>
<tr>
<td>Owner</td>
<td>30.05.2013</td>
</tr>
</tbody>
</table>

### Distribution List

Name: Internal Distribution Only

### Version History

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Version Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Draft 0.1</td>
<td></td>
</tr>
<tr>
<td>1.0</td>
<td>30.05.2013</td>
</tr>
</tbody>
</table>
# OIL-IS-ISMS-COD-1.0 (Procedure for Control of Documents)

## Table of Contents

1. *Introduction* .......................................................................................................................... 4
2. *Key Practices Details* ............................................................................................................ 4
   2.1 Roles and Responsibilities ................................................................................................. 4
   2.2 Structure of ISMS documents .......................................................................................... 4
   2.3 Preparation of Documents .............................................................................................. 5
   2.4 Review and Approval of Documents ................................................................................ 6
   2.5 Issue and Control of Documents ...................................................................................... 6
   2.6 Master List of ISMS Documents ..................................................................................... 7
   2.7 Changes to Documents .................................................................................................... 7
1. Introduction

The purpose of this procedure is to establish effective control over the preparation, authorization, issue, distribution, maintenance, integrity and subsequent change (if any) of documents required by the ISMS, in all process areas. Document Control procedures are applicable to all Information Security Management System (ISMS) documents.

2 Key Practices Details

2.1. Roles and Responsibilities

The key practices and responsibilities are as follows:

<table>
<thead>
<tr>
<th>S.No</th>
<th>Key Practice</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Preparation of Documents</td>
<td>Process owner</td>
</tr>
<tr>
<td>2.</td>
<td>Review and Approval of Documents</td>
<td>Chief Information Security Officer/ Functional Head</td>
</tr>
<tr>
<td>3.</td>
<td>Issue and Control of Documents</td>
<td>Chief Information Security Officer</td>
</tr>
<tr>
<td>4.</td>
<td>Changes to Documents</td>
<td>Process owner</td>
</tr>
</tbody>
</table>

Further, all the ISMS related documentation will be reviewed and approved by the Information Security Council (ISC).

All new issues of ISMS documents as well as revised versions owing to changing practices are initiated, reviewed, approved and issued through the following method.

2.2. Structure of ISMS documents

All ISMS documents contain the following document control information:

- The first page shall contain the company logo and document name.
OIL-IS-ISMS-COD-1.0 (Procedure for Control of Documents)

- The information given in Header and Footer are:
  - Company Name/ logo;
  - Document Title and Document No.;
  - Classification of document;
  - Version No.; and
  - Page No.

- To record the revision history, the following details are also captured in all ISMS documents:

<table>
<thead>
<tr>
<th></th>
<th>Signatures with Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td></td>
</tr>
<tr>
<td>Version</td>
<td></td>
</tr>
<tr>
<td>Classification</td>
<td></td>
</tr>
<tr>
<td>Release Date</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>Review Date</td>
<td></td>
</tr>
<tr>
<td>Author</td>
<td></td>
</tr>
<tr>
<td>Reviewer/ Custodian</td>
<td></td>
</tr>
<tr>
<td>Approved By</td>
<td></td>
</tr>
<tr>
<td>Owner</td>
<td></td>
</tr>
</tbody>
</table>

2.3. Preparation of Documents

All ISMS system documentation that includes ISMS policy, ISMS manual and other relevant documents shall be prepared by the concerned process owner. The details shall be entered in the applicable standard formats. Each document must have the details as mentioned in the section 2.2.

Any new documents that need to be generated shall be identified by the concerned Functional Head / CISO and the activities mentioned above will be executed.
OIL-IS-ISMS-COD-1.0 (Procedure for Control of Documents)

Documents related to ISMS procedures are also controlled by change management.

2.4. Review and Approval of Documents

ISMS system documentation shall be reviewed for adequacy of contents and clarity and also approved before issue.

All documents shall be reviewed by the corresponding process owner(s) and approved by the CISO.

2.5. Issue and Control of Documents

- The original - approved documents shall be maintained by the CISO.
- A soft copy of the document shall be uploaded on the intranet portal. This will enable all employees to access the ISMS documentation.
- “Read-Only” access will be provided for the documents uploaded on the intranet. This will ensure that the documents on the intranet are not tampered / changed by anyone.
- At any given moment, the ISMS document on the intranet will be considered as a “Controlled Copy”. Any print out or downloaded version of the document available on any desktop / server (apart from the one on the intranet) will be considered as “Uncontrolled Copy”.
- The original document of the superseded versions will be stamped as “obsolete”.
- When the documents undergo revision, the revised versions will be verified for completeness and accuracy before issue; the CISO will ensure that the obsolete versions are simultaneously withdrawn from use. The obsolete versions are to be retained for three years.
- Where there is a requirement to issue certain ISMS System Documents to an outside agency the issues will be made after prior approval from the CISO. The copies so issued, will be stamped as “Uncontrolled Copy”.
- External documents are norms relating to ISMS. These documents are controlled by CISO.
2.6. Master List of ISMS Documents

A Master List of ISMS System documents shall be maintained by the CISO in the enclosed format that covers:

<table>
<thead>
<tr>
<th>Document Number</th>
<th>Document Title</th>
<th>Document Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A review and approval of ISMS documentation will be conducted every year or as and when a change is requested. The Master list will also be correspondingly updated.

2.7. Changes to Documents

- Any department / section requiring a change in the ISMS system documents will originate a Change Request Form and forward it to the concerned process owner / CISO.

- A change may be classified as major or minor based on its effect on specifications or the output of the process. It is accordingly affected either as an Amendment (minor) or a Revision (major) as follows:

<table>
<thead>
<tr>
<th>Change Type</th>
<th>Criteria</th>
<th>Changing Version Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minor</td>
<td>Error correction, changes in processes not affecting output specification</td>
<td>Minor number incremented by &quot;0.1&quot;</td>
</tr>
<tr>
<td>Major</td>
<td>Changes that affect output specification</td>
<td>Major portion of version number is incremented by &quot;1&quot; and minor number is initialized to &quot;0&quot;.</td>
</tr>
</tbody>
</table>

- All changes will be subject to the same review and approval process given above.

- The changes will be captured in the version history of each document.
**Document Details**

<table>
<thead>
<tr>
<th><strong>Title</strong></th>
<th>Procedure for Control of Records</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Version</strong></td>
<td>1.0</td>
</tr>
<tr>
<td><strong>Classification</strong></td>
<td>Internal</td>
</tr>
<tr>
<td><strong>Release Date</strong></td>
<td>30.05.2013</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Procedure for control of Oil India records</td>
</tr>
<tr>
<td><strong>Review Date</strong></td>
<td>30.05.2013</td>
</tr>
<tr>
<td><strong>Author</strong></td>
<td>CISO</td>
</tr>
<tr>
<td><strong>Reviewer/ Custodian</strong></td>
<td>CISO</td>
</tr>
<tr>
<td><strong>Approved By</strong></td>
<td>Information Security Council (ISC)</td>
</tr>
<tr>
<td><strong>Owner</strong></td>
<td>CISO</td>
</tr>
</tbody>
</table>

**Distribution List**

<table>
<thead>
<tr>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Distribution Only</td>
</tr>
</tbody>
</table>

**Version History**

<table>
<thead>
<tr>
<th><strong>Version Number</strong></th>
<th><strong>Version Date</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Draft 0.1</td>
<td></td>
</tr>
<tr>
<td><strong>1.0</strong></td>
<td>30.05.2013</td>
</tr>
</tbody>
</table>
Table of Content

1. Introduction ........................................................................................................................ 4
2. Key Practices Details .............................................................................................................. 4
   2.1 Roles and Responsibilities .................................................................................................. 4
   2.2 Procedure in description .................................................................................................... 4
1. Introduction

This procedure helps establish effective control over the Information Security Management System (ISMS) records for identification, storage protection, retrieval, retention time and disposition of records.

This procedure is applicable to ISMS records including but not limited to records of incident / problem management, change management, minutes of Information Security Management Group (ISMG) meetings, equipment maintenance records, backup log register, backup tape movement register, visitor register, etc.

2. Key Practices Details

2.1 Roles and Responsibilities

The key practices and responsibilities are as follows:

<table>
<thead>
<tr>
<th>S.No</th>
<th>Key Practice</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Maintaining the procedure for control of records</td>
<td>Process owner</td>
</tr>
</tbody>
</table>

2.2 Procedure in description

The various records maintained (including their minimum retention periods and the agency responsible for their maintenance) are given in the procedures which form the ISMS.

A Master list of procedures and the corresponding records will be maintained.

Records will be collected, filed, stored and maintained by the concerned Departments in such a way that deterioration, loss or damage is prevented and they can be readily retrieved. They will also be written / entered in a legible manner.
IN-IS-IMS-COR-1.0(Procedure for Control of Records)

Access to the records is available to the concerned Functional Head / Manager only. Access may be given to other personnel on approval from the concerned Functional Head / Manager.

Records of each department will be collected from the operational / functional personnel by the Functional Head / Manager or their representatives. They will be filed sequentially in files. Records will be distributed to all concerned as per the requirements of the respective procedures / Work Instructions, etc.

The files containing records will be stored under lock and key in filing cabinets/ almirahs / cupboards and will be periodically checked for any deterioration and / or damage. The respective process owner will be responsible for key security.

These records (e.g. Training Records, test protocols, etc.) are not controlled by change management, they are the objective proof for performance of demanded actions.