**Information Security Management System (ISMS) Policy**

Doc ID: POL/ISMS

Document Classification: Internal

July 2022

**Document Control Information**

| Document Name | Incident Management Policy and Procedure |
| --- | --- |
| Document ID | {Company}/POL/IMP |
| Document Owner | Information Security Officer |
| Classification | Internal |
| Approved By |  |

| **Authorization** | | | |
| --- | --- | --- | --- |
| **Stakeholders** | **Read Access** | **Write Access** | **Media Type** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

| **Amendment Log** | | | | | |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Modification Date**  **DD MMM YYYY** | **Author (s)** | **Reviewed By** | **Approved by** | **Brief description of the change** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**TABLE OF CONTENTS**

1.0 Introduction 5

1.1 Information Security Definition 5

1.2 Security Policy of {Company} Technologies 5

1.3 Responsibility for Information Security 5

1.4 Applicability of the Policy 6

2.0 Ownership and Maintenance 7

2.1 Policy Owner/ Custodian / Management Representative 7

2.2 Update and Maintenance 7

2.3 Periodic Overview / Framework for Setting Objective and Policy 7

2.4 Document Distribution 7

3.0 ISMS Policy and Objectives 9

3.1 Scope of the ISMS 9

3.2 Information Security Requirements 9

3.3 Objectives 9

4.0 Policy Framework 11

4.1 Information security awareness training 11

4.2 Contracts of employment 11

4.3 Security control of assets 11

4.4 Access Controls 12

4.5 User Access Controls 12

4.6 Computer Access Control 12

4.7 Application Access Control 12

4.8 Computer and Network Procedures 12

4.9 Protection from Malicious Software 12

4.10 Removable Media 12

4.11 Monitoring System Access and Use 12

4.12 Accreditation of Information Systems 13

4.13 System Change Control 13

4.14 Intellectual Property Rights 13

4.15 Governance 13

4.16 Business Continuity 13

4.17 Information Classification, Handling and Retention 14

4.18 Security Incident Management 14

4.19 Physical Security 14

4.20 Data Privacy 14

4.21 ICT Systems Management 14

4.22 Cryptography 15

4.23 Vendor Management 15

5.0 Management Responsibility 16

5.1 Senior Management Commitment 16

5.2 Resource Management 16

6.0 Management Review of the ISMS 17

6.1 General 17

6.2 Review Input 17

6.3 Review Output 17

6.4 Roles and Responsibilities 18

6.5 Continual Improvement Policy 18

6.6 Approach to Managing Risk 19

6.7 Risk Assessment 19

6.8 Internal ISMS Audits 19

7.0 Awareness and Training 20

8.0 Documentation Structure and Policy 20

9.0 Control of Records 20

10.0 Information Systems Security Policy Exception 21

10.1 Introduction 21

10.2 Procedure 21

11.0 Information Systems Security Policy Violations 21

11.1 Introduction 21

11.2 Procedure 22

12.0 Reference Documents 22

# Introduction

{Company} is setting up an Information Security Management System (ISMS) across the organization, in compliance with ISO/IEC 27001:2013 standard, validated by an external third party, to ensure effective adoption of Information Security best practices and assurance to clients and stakeholders.

This Information Security (IS) Policy is intended to provide management direction and support for Information and Cyber Security to employees and stakeholders for {Company}. This policy indicates and defines management support for, and commitment to the principles of Information Security. The ISMS will be managed through the issue and maintenance of, related, documented policies and procedures and the implementation of associated process controls and guidelines, across the organization.

## Information Security Definition

“Information Security protects information from a wide range of threats to ensure business continuity, minimize business damage and maximize return on investments and business opportunities.”

Information Security is driven by the following control objectives across IT and business processes in the organization:

* Confidentiality: Ensure the protection of sensitive information and information assets from unauthorized access.
* Integrity: The accuracy and completeness of information as well as to its validity in accordance with business values and expectations should be maintained
* Availability: Information should be available as and when required by the business. The objective for maintenance of the confidentiality, integrity and availability should be ensured through appropriate controls, on the people, process and technologies in the organization.

## Security Policy of {Company} Technologies

Information security is monitored and implemented by C.T.O.

* The Information Security Policy states:

*“*{Company} *is committed to securing organizational information assets, including data of all business partners and customers associated with it.*

* {Company} *will ensure that appropriate information security controls are applied and integrated to ensure information protection from threats to confidentiality, integrity and availability thereby enhancing the confidence of and adding value to all its stakeholders.*
* {Company} *Management assures all stakeholders that the ISMS will be continually monitored to ensure effectiveness and compliance.”*

## Responsibility for Information Security

All employees and other external parties who require access to the organization’s information and associated assets are responsible for ensuring that this policy is adhered to. Management at all levels is responsible for ensuring that the information users are aware of and adhere to this policy.

## Applicability of the Policy

This policy applies to all the employees, apprentice, contractors, customers, consultants and other individuals affiliated with external parties who have access to the organization information. Throughout this document, the word “user” is used to collectively refer to all such individuals.

# Ownership and Maintenance

## Policy Owner/ Custodian / Management Representative

The Information Security Officer is the owner of ISMS Overview Policy, Information Security Policies and Procedures.

The Information Security Officer shall have overall authority and responsibility for the implementation and management of the Information Security Management System, specifically:

* The identification, documentation and fulfillment of the information security requirements.
* Implementation, management and improvement of risk management process.
* Integration of processes.
* Compliance with statutory, regulatory and contractual requirements.
* Reporting to top management on performance and improvement.

## Update and Maintenance

The Information Security Officer being the policy owner, is responsible for updating of contents and overall maintenance of the policy.

## Periodic Overview / Framework for Setting Objective and Policy

* The Information Security Officer is responsible for the maintenance and review of the policy according to a defined review process. This process will ensure that a review takes place in response to any changes affecting the basis of the original risk assessment, e.g., significant security incidents, new vulnerabilities or changes to the organizational or technical infrastructure.
* ISMS objectives shall be documented, together with the details of how they will be achieved. These will be reviewed on an annual basis to ensure that they remain valid.
* In accordance with ISO/IEC 27001:2013, the control objectives and policy statements detailed in Annex A of the standard shall be adopted where appropriate by the organization.
* The policy shall be reviewed, considering the outcome from risk assessment or every year or at the time of any significant change in existing Information System environment affecting policies and procedures, whichever is earlier, by the Management Representative. The review reports shall be submitted to Management.
* All policies and supporting documents would expire in 3 years if not reviewed and hence they would mandatorily need to be reviewed and updated within 3 years timeframe and revalidated.

## Document Distribution

This document is for restricted distribution only, as it contains {Company} strategy for the disciplinary process for the users. Therefore, the policy should be distributed on a need-to-know basis only.

In addition to this, a hard copy of the documentation should be maintained with the Information Security Officer in an access controlled and secure environment.

Should the organization receive a request from the customer, the relevant and appropriate section of the policy document may be shared after seeking approval from the CEO, HR and Department Head.

Should the organization receive a request from any law enforcement agency, the Management Representative after seeking approval from CEO, HR and Legal may review and release the policy document.

# ISMS Policy and Objectives

## Scope of the ISMS

For the certification within the organization, the boundaries of the Information Security Management System has been defined.

Refer to the document “ISMS Scope” for more details.

## Information Security Requirements

A clear definition of the requirements for information security will be agreed and maintained with the business so that all Information Security Management System activity is focused on the fulfillment of those requirements. Statutory, Regulatory and Contractual requirements will also be documented and will be the input to the process. Specific requirements concerning the security of new or changed systems or services will be captured as part of the design stage of each project.

It is the principle of {Company} Information Security Management System that the controls implemented are driven by business needs and this will be regularly communicated to all staff via various communication channels as defined in the “Communication Procedure”.

## Objectives

The purpose of the ISMS is to ensure that the organization can meet its defined business objectives and comply with polices in the face of potential and actual security incidents. This section sets out what are the primary business objectives related to security so that a clear relationship can be established between these and the objectives of the ISMS.

These business objectives for security are authorized by the Management and shall be implemented and maintained by the Information Security Officer.

Information and information systems are considered the foremost important factor in continuing the day to day functions effectively. Supporting the objectives of the organization is committed to secure the information, the information systems and the network infrastructure by adapting to the following principles:

* Protect the information and the network infrastructure against external or internal threats.
* Provide a minimum level of access between information systems and the users on a “need to know” basis.
* Classify the information according to its criticality to protect it against unauthorized modifications or disclosure.
* Adopt a set of standards, guidelines and procedures to ensure the security of information, the information systems and the network infrastructure.
* Conduct security awareness training within the organization to educate the users about the best security practices when working with information and information systems.
* Conduct continuous risk assessment, risk analysis and risk management procedures to information and information systems.
* Ensure that information and information systems are protected against unauthorized access.
* Ensure that users comply with all the local and cyber laws and information security policy about information and information systems.
* Protect the users and the organization from any inappropriate use that would expose the organization to risks including virus attacks, compromise of network systems and services and any other legal issues.

{Company} has set the following major business objectives related to security:

**Objective 1 – Maintain a suite of security policies**

{Company} shall maintain an information security policy and associated policies required for ensuring its people, process, information and technologies are not at risk of security compromise. The information security policy shall be aligned to the ISO/IEC 27001 best-practice standard for information security. Compliance with these policies shall be mandatory for all employees and third parties who manage or access {Company} systems. These policies shall be reviewed on an annual basis and / or whenever there are significant changes by the Information Security Officer.

**Objective 2 – Maintain security awareness and education to staff**

For the year < mention the year> -() % of employees not trained - Target is ()%

All the employees shall receive security awareness and education training annually. The sessions must update employees on their obligations to security while working at {Company}, making them aware of new security threats, current policy, updates to regulatory requirements and any changes to policy which may affect their working environment. Extra, more targeted sessions may also be delivered upon request or if the need arises at the discretion of the Management team.

**Objective 3 – Manage and reduce critical security incidents**

For the year < mention the year> – Critical security incident – Target is <=2

**Objective 4 – Execute BCP Tests on a timely basis**

For the year < mention the year> – BCP Test executions on-time as per the annual scheduled plan

# Policy Framework

## Information security awareness training

Information security awareness training will be included in the staff induction process. An on-going awareness program will be established to ensure that staff awareness is refreshed and updated annually.

* Users shall receive appropriate training on security requirements in use/development of information systems, applications and other information processing facilities.
* Users shall also be made aware of their security responsibilities and disciplinary process, which can be initiated against them in case of any violations to the organization’s policies and procedures.
* The HR department in co-ordination with the IT Team and Management Representative is responsible for designing and delivering security awareness sessions to existing employees regularly.
* Senior Management (Department Head / Delivery Head / Project Managers) should address “Information Security” during their interactions with the users.
* Posters and handouts may be used for creating security awareness among employees.
* The induction training for all new joinee’s should cover a session on introduction to Information Security Practices.
* Training should cover the following topics, but not limited to:
  + Basics of Information Security
  + Organizational Policies and Procedures
  + User Do’s and Don’ts
  + Disciplinary Process
  + Evaluations and suggestions should be sought after every training session
* Refresher programs should be conducted periodically by the Management Representative to reinforce security awareness.
* Information Security awareness should also be disseminated through the available mediums of communication.

## Contracts of employment

Security requirements will be addressed at the recruitment stage and all contracts of employment will contain a confidentiality clause. Security requirements will be included in the job definition. This is documented in the Personnel Security Procedure.

## Security control of assets

Every asset (hardware, software, application or data) will have a named custodian who will be responsible for the security of that asset. This is documented in the Information Classification Procedure.

## Access Controls

Access to the organization’s systems and information must be controlled to protect its confidentiality, integrity and availability. Accordingly, access is restricted to those with a ‘need to know’ and is reviewed periodically to ensure appropriate access is maintained. Access credentials must meet specific minimum requirements, depending on the subject system, to reduce the risk of unauthorized access.

Only authorized personnel who have a business need will be given access to restricted areas containing information systems. This is documented in the Information Classification Procedure.

## User Access Controls

Access to information will be restricted to authorized users who have a business need to access the information.

## Computer Access Control

Access to computer facilities will be restricted to authorized users who have a business need to use the facilities.

## Application Access Control

Access to data, system utilities and program source libraries will be controlled and restricted to authorized users who have a business need to use the applications. Authorization to use an application will depend on the availability of a license from the supplier.

## Computer and Network Procedures

Management of computers and networks will be controlled by standard procedures that have been authorized by the organization. This is documented in the Network Security Policy.

## Protection from Malicious Software

The organization will use software countermeasures and management procedures to protect itself against the threat of malicious software. All employees are expected to adhere fully to this policy. Employees must not install software on the computing assets without following the defined process. Staff breaching this requirement may be subject to disciplinary action.

## Removable Media

Removable media containing software or data from external sources, or that have been used in external equipment must be fully virus checked before being used on the equipment. Users breaching this requirement may be subject to disciplinary action. This is documented in Computing Environment, Network Security Policy and Incident Management Policy.

## Monitoring System Access and Use

An audit trail of system access and use must be maintained and reviewed regularly.

## Accreditation of Information Systems

The organization will ensure that all new information systems, applications and networks include security policy and plan and are approved before they commence operation. New information systems within the scope must be penetration tested and vulnerability scanned, with issues remediated before going live.

## System Change Control

Changes to the information systems, applications or networks must be reviewed and approved. This is documented in the Change Management Policy.

## Intellectual Property Rights

The organization will ensure that all information products are appropriately licensed and approved by the management.

## Governance

{Company} operates in an environment where it must: comply with national and international laws, consistently demonstrating effective ISMS to its external auditors; and are able to show to the customers that its contractual security obligations are being met. Additionally, as threats constantly change and develop, so must the controls whilst at the same time continuing to support business aims.

Therefore, ISMS must be kept under regular review to ensure that the policies and controls in place continue to support business aims by adapting to the changing threat landscape, incorporating any statutory or regulatory requirements is considered when applying and managing controls; that consequential risk are identified and appropriately managed; and that any changes to the legal or regulatory environment are incorporated. For these reasons, {Company} monitors the effectiveness of its controls by conducting tests against its infrastructure, for example, penetration or vulnerability testing; by collecting information on policy compliance, such as endpoint encryption and anti-virus status; by conducting audit across the ISMS by its internal teams; and by exercising its contingency and response plans.

The results of these governance activities will be contained in reports distributed to the appropriate teams and their management and it is the responsibility of the control owners to ensure that any weaknesses are mitigated and managed. This is documented in the Compliance and Internal Audit Procedure.

## Business Continuity

The implementation of an effective Business Continuity policy ensures preparations are made to identify risks which may affect the organization’s ability to operate during an incident and recover quickly in the aftermath. All employees must ensure they understand the business continuity process and their place in it. Business Continuity plans and processes must be regularly reviewed and tested to ensure effectiveness. This is documented in the BCP-DRP Procedure.

## Information Classification, Handling and Retention

Information assets created, stored and used within the organization have value, which must be identified by the asset owner to allow the appropriate security controls to be applied. Additionally, information processed for customers must be classified according to its value to the customer.

All employees are required to protect information according to the data classification assigned to it. Access to all classified information is based on the “need-to-know” principle. Although people might be authorized to access information, they should only access data when strictly required.

## Security Incident Management

A risk-based approach to security-focused on supporting business aims, such as that implemented by the organization, results in the likelihood that a security incident will occur at some point. Therefore all employees must ensure that they know how to identify and report a security incident and must be thoroughly familiar with their involvement in the incident management process. Incident Management processes must be in place and tested.

## Physical Security

Information and assets at the facilities must be classified according to their organization value and appropriately protected. Physical Security Policy defines guidelines for the identification, assessment and management of physical security risks and the implementation of several security zones within the facility.

## Data Privacy

Employees handle a variety of personal information for both other organization employees and customers. In some cases, this personal information may fall into the category of sensitive information, which requires increased levels of protection. In all circumstances, personal information and sensitive personal information must be processed and stored in accordance with organization’s policies and any local legislation.

Management Representative / Data Privacy Officer maintains a Privacy Legislation Framework to meet regulatory requirements for data privacy. The Privacy Legislation Framework covers relevant privacy legislation for the organization as a data controller and / or data processor. This is documented in the Data Privacy Policy.

## ICT Systems Management

ICT Systems includes all ICT systems used by the organization. Organization’s requirements for ICT system installation and maintenance can be found in Information Classification Policy.

Customer-owned systems are managed and maintained by the customer; this responsibility includes information security. In case employees are required to access such systems, customer’s security requirements apply.

## Cryptography

The organization uses cryptography to protect physical and logical assets. Cryptographic solutions must be employed correctly for them to be effective and cryptographic keys must be managed to ensure their availability. The requirements for cryptography are contained in several policies such as Cryptography Policy.

## Vendor Management

Organization’s supply chain constitutes a risk due to the reliance on third-party implementing appropriate controls to protect services and information. Organization’s vendor on-boarding process must include an information security assessment which varies in detail depending on the goods or services to be provided or the level of physical or logical access provided to the vendor. Additionally, a “Right to Audit” clause should be included in vendor contracts. Vendor contracts should also include a set of minimum expected security requirements for protecting organization assets and information and an obligation for the vendor to inform if they suffer a successful cyber-attack. This is documented in External Party Management.

# Management Responsibility

## Senior Management Commitment

* {Company}’s Management shall provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS by:
  + Establishing an Information Security Policy
  + Ensuring that information security objectives and plans are established
  + Establishing roles and responsibilities for information security
  + Communicating to the organization the importance of meeting information security objectives and conforming to the Information Security Policy, its responsibilities under the law and the need for continual improvement
  + Providing sufficient resources to develop, implement, operate and maintain the ISMS
  + Deciding the acceptable level of risk
  + Risk Management and Evaluation (risks are derived from the asset register (i.e., the dependencies of the risk within the project), the context (i.e., the external and internal issues/parameters))
  + Conducting management reviews of the ISMS
* The reviews would be done at the management level at least once every three months
* Implementation of new information processing facilities should be approved and authorized by Management Information Security Forum (MISF)

## Resource Management

{Company} shall determine and provide the resources needed to:

* Establish, implement, operate and maintain ISMS
* Ensure that information security procedures support the business requirements
* Identify and address legal and regulatory requirements and contractual security obligations
* Maintain adequate security by the correct application of all implemented controls
* Carry out reviews when necessary, and to react appropriately to the results of these reviews
* Where required, improve the effectiveness of the ISMS

# Management Review of the ISMS

## General

{Company} Management shall review the organization’s ISMS at planned intervals to ensure its continuing suitability, adequacy and effectiveness. This review shall 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 shall be clearly documented and records shall be maintained.

## Review Input

The input to {Company} management review shall include information on:

* Status of actions from previous management reviews
* Changes in External and Internal Issues that are relevant to the information security management system
* Feedback on the information security performance, including trends in:
  + Non-conformities and corrective actions
  + Monitoring and measurement results
  + Audit results
* Fulfillment of information security objectives
* Feedback from interested parties
* Results of risk assessment and status of the risk treatment plan
* Opportunities for continual improvement

## Review Output

The output of the {Company} management review shall include any decisions and actions related to the following:

* Improvement of the effectiveness of the ISMS
* Modification of procedures that affect information security, as necessary, to respond to internal or external events that may impact on the ISMS, including changes to:
  + Business requirements
  + Security requirements
  + Business processes affecting the existing business requirements
  + The regulatory or legal environment
  + Levels of risk and/or levels of risk acceptance

## Roles and Responsibilities

* There are several management roles that correspond to the areas defined within the scope set out above. Full details of the responsibilities associated with each of the roles and how they are allocated are given in a separate document (ISMS Policy Organization Structure and Roles and Responsibilities)
* It is the responsibility of the Management Representative to ensure that everyone understands the roles they are fulfilling and that they have appropriate skills and competence to do so.

## Continual Improvement Policy

{Company} Policy with regard to Continual Improvement is to improve the effectiveness of the ISMS implemented through the following:

* Enhancing current processes to bring them into line with good practice as defined within ISO/IEC 27001
* Achieving ISO/IEC 27001 certification and maintain it on an on-going basis
* Making information security processes and controls more measurable to provide a sound basis for informed decisions
* Reviewing relevant metrics on an annual basis to assess whether it is appropriate to change them, based on collected historical data
* Obtaining ideas for improvement and documenting them in a Continual Improvement Plan
* Reviewing the Continual Improvement Plan at regular management meetings to prioritize and assess timescales and benefits
* Continually improving the effectiveness of the ISMS

Ideas for improvement may be obtained from any source including employees, customers, suppliers, risk assessments, audits and service reports. Once identified; they shall be added to the Continual Improvement Plan and evaluated by Management Representative for Continual Service Improvement.

As part of the evaluation of proposed improvements, the following criteria may be used:

* Cost
* Business Benefit
* Risk Assessment
* Implementation timescale
* Resource requirement

If accepted, the improvement proposal will be prioritized and implemented as per the plan.

## Approach to Managing Risk

Risk management will take place at several levels within the organization, including, but not limited to:

* Management planning – risk to the achievement of objectives
* Information security and IT service continuity risk assessments
* Assessment of the risk of changes via the change management process
* As part of the design and transition of new or changed services
* As derived from the asset inventory and the context

High-level risk assessments shall be reviewed on an annual basis or upon significant change to the business or service provision.

## Risk Assessment

A risk assessment process will be used, which is in line with the requirements and recommendations of ISO/IEC 27001, the International Standard for Information Security. This is documented in the Risk Assessment and Risk Management Procedure.

## Internal ISMS Audits

Internal Audit Team of {Company} shall conduct internal ISMS audits at planned intervals to determine whether the control objectives, controls, processes and procedures of its ISMS:

* Conform to the requirements of this standard and relevant legislation or regulations
* Conform to the identified information security requirements
* Are effectively implemented and maintained
* Perform as expected

An audit program shall be planned, taking into consideration the status and importance of the processes and areas to be audited, as well as the results of previous audits. The audit’s criteria, scope, frequency and methods shall be defined. Selection of auditors and conduct of audits shall ensure objectivity and impartiality of the audit process. Auditors shall not audit their own work.

The responsibilities and requirements for planning and conducting audits, and for reporting results and maintaining records shall be defined in Internal Audit Management Procedure.

{Company}’s management responsible for the area being audited shall ensure that actions are taken without undue delay to eliminate detected non-conformities and their causes. Improvement activities shall include the verification of the actions taken and the reporting of verification results.

# Awareness and Training

Information Security can only be successful if all employees are able to appreciate the importance of information that is used in their day to day operations and help in their protection. In order to ensure that the employees are adequately made aware of the acceptable and non-acceptable practices, suitable awareness training, visual aids, employee communication, etc. would be provided. Further, it would be the responsibility of Department Head to ensure that the communication to their teams is complete and the ownership is clearly established. The time and commitment from senior management would also be devoted to furthering awareness across the organization.

{Company} shall ensure that all staff involved in Information Security is competent on the basis of appropriate education, training, skills and experience.

The skills required shall be determined and reviewed regularly, together with an assessment of existing skill levels. Training needs shall be identified and a plan maintained to ensure that the necessary competencies are in place.

Training, education and other relevant records shall be kept by the HR department. Individual skill levels / competency details shall be maintained by Management Representative.

# Documentation Structure and Policy

All information security policies and plans must be documented. This section sets out the main documents that must be maintained in each area. Details of documentation conventions and standards are defined in Control of Document Procedure.

A number of core documents have been created and will be maintained as part of the ISMS. They are uniquely numbered and the current versions are tracked in Document Control Matrix.

# Control of Records

The keeping of records is a fundamental part of the ISMS. Records are key information resources and represent evidence that processes are being carried out effectively.

The controls in place to manage records are defined in the document Controls of Records Procedure.

# Information Systems Security Policy Exception

## Introduction

There may be instances where there is a justifiable business need to perform actions that are in conflict with {Company}’s Information Systems Security Policies and Procedures. {Company} recognizes that policies cannot be created and enforced which address all business issues. In order to provide flexibility in such instances, this component of Information systems security policy should be referred to get details of actions that are required to obtain a waiver from compliance to a specific policy.

Any person who identifies an exception to Information System Security Policies that must occur in order to successfully complete business operations must immediately inform his/her immediate reporting manager, who shall initiate immediate action to the Management Representative or the MISF, that may be required to obtain a waiver from compliance to a security policy.

## Procedure

Requests for exceptions to policies must have a justifiable business case documented and must have the necessary approvals. Exceptions must be approved by the Management Representative.

Once approved, exceptions to policy will be valid for a pre-decided period after which it must be re-evaluated and re-approved.

If policy exceptions are likely to circumvent existing internal controls, then “Mitigating Controls” or “Compensating Controls” must be implemented and followed. The Management Information Security Forum (MISF) must be involved in all instances where internal security controls are bypassed.

# Information Systems Security Policy Violations

## Introduction

Violations of this security policy may include but are not limited to any act that:

* Does not comply with the requirements of this policy.
* Exposes {Company} to actual or potential loss through the compromise of security.
* Involves the disclosure of confidential information or the unauthorized use of {Company}’s information.
* Results in loss of {Company}’s information.
* Involves the use of the hardware, software or information for unauthorized or illicit purposes which may include violation of any law, regulation or reporting requirements of any law enforcement or government body.
* Violates any laws or regulations which may be introduced by the Government of India from time to time.

Any person who becomes aware of any loss, compromise, or possible compromise of information, or any other incident which has information security implications, must immediately inform his/her reporting manager and Management Representative, who shall initiate immediate action to prevent further compromise or loss.

## Procedure

The reporting manager, along with Management Representative, shall be responsible for getting the violation investigated and taking disciplinary action as deemed appropriate. All incidents of security violation shall be dealt with in a manner specified and defined in the Incident Management Policy and Personnel Security Procedure.

The Management Representative shall report the details of the violation to the relevant Asset Owner, if any, who will determine if the violation has had an impact on the integrity of the information.

The Management Representative, as deemed appropriate, shall be responsible for coordinating appropriate action to prevent a recurrence of the violation or to focus security education efforts in the particular area.

# Reference Documents

* ISO 27001:2013
* Statement of Application for ISO27001:2013
* Risk Assessment and Risk Management Procedure
* Roles and Responsibilities
* ISMS Policy Organization Structure
* Skill Competency Matrix
* Controls of Records Procedure
* Continual Improvement Plan
* Internal Audit Management Procedure
* Control of Document Procedure
* Document Control Matrix
* Incident Management Policy