



Information Security Policy Document

Version _____

Revision History

Prepared / Updated By	Reviewed By	Approved By	Owner	Version	Date of Approval	Date of Implementation

Changes made (from previous version)

INFORMATION SECURITY POLICY DOCUMENT

Table of Contents

1	Introduction	4
2	Objective	4
2.1	Scope of Policy	4
2.2	Establish Prudent Practices.....	5
2.3	Maintain Technological Innovation	5
2.4	Train [REDACTED] Computer Users.....	5
2.5	Staff Responsibilities	5
2.6	Policy	5
3	Information Security Policy	6
3.1	Information Security Organization.....	6
3.2	Asset classification and control.....	6
3.3	Personnel security.....	6
3.4	Physical and environmental security	6
3.5	Communications and operations maintenance.....	6
3.6	Access control	6
3.7	Password Policy.....	7
3.8	Surveillance System Audit policy	7
3.9	Violation and legal action	7
3.10	Clear Desk / Clear Screen Policy.....	7
3.11	Physical Access.....	8
3.12	Employee code of conduct	8
3.13	Document Security.....	8
3.14	Security Risk Assessment	8
3.15	Data Back up	9
3.16	Logical Access.....	9
3.17	Remote Access	9
3.18	Internet Access.....	9
3.19	System development and maintenance	9

3.20	System and Network Security	10
3.21	Vulnerability Scanning	11
3.22	Outsourcing policy	11
3.23	Business continuity management	11
3.24	Change management	11
3.25	Compliance	11
3.26	Internal Audit	12
3.27	Monitoring Usage	12
3.28	Information Security Services	13
3.29	All activities on Information Systems are constantly monitored.....	13
3.30	Sub Policies	13
3.30.1	Acceptable Asset use policy	13
3.30.2	Network Acceptable Use Policy	13
3.30.3	Software Usage Policy.....	14
3.30.4	E-MAIL Policy.....	14
4	Enforcement	15
5	Information Security Declaration.....	16

INFORMATION SECURITY POLICY DOCUMENT

1 Introduction

The Chief Executive Officer of the [REDACTED] has issued an Information Security Policy; the policy defines the [REDACTED] security objectives, and its expectations about how staff will protect the [REDACTED] information.

The [REDACTED] regards its information as a valuable asset. The computers and networks that process [REDACTED] information are critical to its business operations. All [REDACTED] staff must comply with the information security Policy in order to achieve the following:

- Protect the investment and the good name of the organization.
- Safeguard the information contained within these systems.
- Reduce business and legal risk.

Protection will be provided through cost-effective combinations of hardware, software and procedures.

2 Objective

The objective of information security is to ensure the responsible use of [REDACTED] public and private data networks and IT resources. (Refer to acceptable Use Policy 3.25.1). Implementation of Security Policy aims to guarantee the Operational continuity and minimize business damage by preventing, controlling, and minimizing the impact of security incidents. This can be accomplished in a number of ways enlisted in the following section.

2.1 Scope of Policy

- All information travelling over the [REDACTED] networks or stored or processed on its servers and workstations.
- All application systems used by the [REDACTED] to process and store its information and information entrusted to it by third parties.
- All computers, servers, workstations, communications equipment and their associated software that are used to deliver the above systems or are connected to them regardless of the physical location of the equipment.
- All personnel who are responsible for developing, implementing, maintaining, operating and using any of the above include the [REDACTED] staff and any contractors, consultants or other third parties employed to work on them.

2.2 Establish Prudent Practices

Establishment of prudent practices will allow us to provide a foundation for security. Many security problems can be solved through the use of prudent practices. We will actively look for problems and situations where the establishment of policy, procedures, and strategies that support a secure posture can be implemented.

2.3 Maintain Technological Innovation

Security technology is rapidly changing. As new threats to information resources arise, it is crucial to implement technological solutions that can shield organizational business resources. It is important to maintain an awareness of the emerging security technologies and develop solutions that are both cost effective and based on current technology.

2.4 Train [REDACTED] Computer Users

Employees play a key role in the protection of [REDACTED] information. Through training and education of information security a high level of awareness can be maintained. This awareness will ensure that [REDACTED] employees can adequately protect their information and are aware of the company rules & regulations.

2.5 Staff Responsibilities

- a) Every staff member of [REDACTED] is RESPONSIBLE for adhering to Information Security Policy.
- b) Users are responsible for protecting any computer equipment issued to them by the [REDACTED].
- c) The [REDACTED] strongly supports strict adherence to software licensing agreements and software copyright holder notices. No unlicensed software may be used on any of the [REDACTED] equipment for processing [REDACTED] information. Anyone taking copies of software or other copyright material that is under the [REDACTED] control must comply with the vendors license agreements and copyright notices.

2.6 Policy

The purpose of this policy is to protect [REDACTED] information assets and intellectual property from all threats, whether internal or external, deliberate or accidental. This policy is approved and supported by [REDACTED] and endorsed by top management. All managers and information

<u>INFORMATION SECURITY POLICY DOCUMENT</u>

Security Officers (ISO) are directly responsible for implementing this policy within their respective business areas.

3 Information Security Policy

It is the policy of [REDACTED] to create and maintain this Information Security Policy to provide management support for Information Security principles, and unambiguously demonstrate to stakeholders the management commitment to Information Security.

3.1 Information Security Organization

It is the policy of [REDACTED] to maintain an Information Security Management System to manage all facets of the Information Security process. The ISMS should be maintained by the IS department.

3.2 Asset classification and control

It is the policy of [REDACTED] to evaluate risks to all corporate assets, tangible and intangible. It is also the policy of [REDACTED] to adopt appropriate controls for the mitigation of risks keeping the asset value in sight.

3.3 Personnel security

It is the policy of [REDACTED] to ensure that all employees are qualified to perform the roles to which they have been assigned in contrast of using IT resources, which include use of Internet, Emails, Accessing database and publishing websites.

3.4 Physical and environmental security

It is the policy of [REDACTED] to ensure that all assets are located in a physically and environmentally secure environment.

3.5 Communications and operations maintenance

It is the policy of [REDACTED] to ensure that all standards, guidelines, and procedures exist to maintain confidentiality, integrity, and availability of information at all times.

3.6 Access control

It is the policy of [REDACTED] to ensure that only authenticated entities are granted access to [REDACTED] information assets. It is also the policy of [REDACTED] to ensure that

Verify Version Before Use

Copyright © [REDACTED] All rights reserved. Unauthorized copy or use of this document is strictly prohibited

		Version: 1.1 RESTRICTED
<u>INFORMATION SECURITY POLICY DOCUMENT</u>		

authenticated entities are only granted access to information to which they are authorized. The default access control policy should be to deny all unless explicitly authorized.

3.7 Password Policy

Users must protect the confidentiality of their passwords of root and user-level accounts, web accounts, e-mail accounts and all other login accounts through the use of strong passwords that cannot easily be guessed or otherwise compromised.

3.8 Surveillance System Audit policy

Internal audit of CMC must be conducted twice in a month by the Audit Team (mentioned in SOP of CMC) to check the fitness of alarms and cameras, recordings of the cameras (14 days of camera recordings must be maintained) and any other access control mechanism for physical security.

3.9 Violation and legal action

- a) Anyone who becomes aware of an incident that indicates a breach of information security must report it immediately to the help desk.
- b) Users must cooperate in any security breach investigation.
- c) In accordance with established practices and (Local) laws regarding computer and information property, anyone found to be abusing or misusing computer resources and network may be subject to disciplinary action up to and including expulsion from the and/or to any other legal action.

3.10 Clear Desk / Clear Screen Policy

- a) When equipment is no longer in use, for example office systems at the end of the working day, it must be logged off and protected from unauthorized use.
- b) All portable equipment e.g. laptops must be switched off or soft locked at the end of each working day. To minimize the risk of theft and potential loss of personal and sensitive information, the portable equipment must be locked out of sight or otherwise secured overnight.
- c) Secure storage must be provided for keys to desks, cabinets, safes and similar storage. Records of digital lock combinations and similar sensitive information must be stored securely. Documented procedures must be implemented for the handling and secure storage of keys. All the Keys to be tagged accordingly.

Verify Version Before Use

Copyright © All rights reserved. Unauthorized copy or use of this document is strictly prohibited

		Version: 1.1 RESTRICTED
<u>INFORMATION SECURITY POLICY DOCUMENT</u>		

- d) The working hours when not in use and outside the working hours , documents, papers, diskettes, portable computer equipment, mobile telephones and similar items, must be stored in locked drawers or cabinets.
- e) Floor areas must be kept clear of boxes, packaging, spare equipment etc., to reduce the risk to personnel during emergency evacuation and at other times,
- f) Confidential correspondence must not be placed in out-trays after the last collection of the day. Confidential information must not be left unattended on unsecured FAX machines, printers or photocopier.

3.11 Physical Access

It is the policy of [REDACTED] to require adequate physical security for all information assets. Physical structures should be secured from both covert and overt penetration. Physical access should be controlled by at a minimum single-factor authentication.

3.12 Employee code of conduct

Every worker at [REDACTED] no matter what their status (employee, contractor, consultant, temporary, etc.) -- must comply with the information security policies found in this and related information security documents. Workers who deliberately violate this and other information security policy statements will be subject to disciplinary action up to and including termination.

3.13 Document Security

The document security includes the following:

- Employees at [REDACTED] should make sure that official documents are easily located, accessed and maintained whilst ensuring confidentiality and integrity of information.
- Employees must ensure that official records are disposed off in an appropriate manner and in accordance to their content and function.
- Documents must be classified into levels (Unclassified, Restricted, and Secret).

3.14 Security Risk Assessment

The Security Risk Assessment is a method to determine that the cost of a countermeasure is commensurate with the identified risk as well as identifying the assets that are at most risk. [REDACTED] shall perform risk assessment of identified assets at regular intervals.

		Version: 1.1 RESTRICTED
<u>INFORMATION SECURITY POLICY DOCUMENT</u>		

3.15 Data Back up

Regular backups are an essential part of using computer systems within the practice. If the computer system fails for any reason with loss of information, it is the backup that will ensure that any loss is kept to a minimum. [REDACTED] shall perform weekly backups of critical devices like mail servers, core firewalls, SAN etc on SAN. Testing backups is important for the surety of their perceived availability whenever they are invoked. Hence testing of the backups will be carried out once in a year and the report will be submitted for an appropriate action.

3.16 Logical Access

It is the policy of [REDACTED] to practice role based logical access control. Authorization levels will be based on job requirements and specified in job descriptions.

3.17 Remote Access

It is the policy of [REDACTED] to limit remote access to users with genuine requirements to ensure confidentiality, integrity, and continued availability of the [REDACTED] IT infrastructure. Determination of legitimate requirements should be at the discretion of the Information Security department. It is the policy of [REDACTED] that any employee accessing the internal services (except email) of [REDACTED] will have to use SSL-VPN (Secure Web-Based VPN) service. It is important to note that the owner of a particular service is responsible for deciding either to publish or not to publish any service over the internet.

3.18 Internet Access

It is the policy of [REDACTED] that an employee cannot use modem, dongle or any other device to access internet (while in the premises of [REDACTED] bypassing the internal network of [REDACTED] Exceptions are for those employees who have taken approval from CISO/ED with viable justification. Violation of this policy clause will result in disciplinary action as required.

3.19 System development and maintenance

It is the policy of [REDACTED] to ensure that development and maintenance efforts do not interfere with confidentiality, integrity, or availability of production systems.

		Version: 1.1 RESTRICTED
<u>INFORMATION SECURITY POLICY DOCUMENT</u>		

3.20 System and Network Security

Violations of system or network security by staff or clients are prohibited, and may result in criminal and civil liability. [REDACTED] will investigate incidents related to system and network security, and may involve and will cooperate with law enforcement agencies if a criminal violation is suspected.

[REDACTED] may implement technical mechanisms to prevent or detect behavior which breaches this policy, and may cooperate with network service providers to detect or control system or network security violation. Examples of system or network security violations include, but are not limited to the following:

- a) Unauthorized access to or use of data, systems or networks, including any attempt to probe, scan, disable or test the vulnerability of a system or network or to breach security or authentication measures without the express authorization of [REDACTED] management, and where an asset is not fully managed by [REDACTED] (e.g.: co-located equipment / servers), asset owner.
- b) Unauthorized monitoring of data or traffic on any network or system without the express authorization of [REDACTED] management, and the owner of the system or data.
- c) Intentional or otherwise interference with service to any user, host or network including, but not limited to, mail “ bombing”, flooding, broadcast attacks, and attempts to overload or disable a system: whether the system is within the [REDACTED] network or not.
- d) Forging of any TCP-IP packet header or any part of the header information in an electronic mail or a newsgroup posting.
- e) The storage or intentional propagation of viruses, Trojans or other maleficent code.
- f) The deliberate removal of audit trails or other security related information.
- g) Staff should endeavor to inform the Chief Information Security Officer (CISO) of any identified or suspected security violations. Of particular note, staff should alert the CISO of attempts to gain access to or knowledge of systems via “Social Engineering” attacks that may resemble telephone calls or emails that appear to be from [REDACTED] clients, service providers or staff.
- h) All reasonable efforts should be made by [REDACTED] staff to ensure that system and infrastructure related changes have been through an appropriate change control process as per the [REDACTED] Security policy, Changes that in some way effect the Interaction between [REDACTED] security zones are of particular concern.
- i) Indirect or attempted violations of the policy, and actual or attempted violations by third party on behalf of an [REDACTED] staff member, shall be considered violation of the policy by such staff member.

Verify Version Before Use

Copyright © [REDACTED] All rights reserved. Unauthorized copy or use of this document is strictly prohibited

		Version: 1.1 RESTRICTED
<u>INFORMATION SECURITY POLICY DOCUMENT</u>		

- j) Complaints regarding Illegal Use or system or network security issues should be directed to the Information Security committee or helpdesk (111).

3.21 Vulnerability Scanning

Parties (Internal or external) that are supposed to perform the scanning activity are required to get the written scanning plan approval from the management. The vulnerability scan should include details of the scanning activity from all aspects. Network performance and/or availability may be affected by the scanning hence management should ensure appropriate measures for the continuity of critical business operations.

3.22 Outsourcing policy

The commercial benefits of outsourcing business functions must be balanced against the commercial and information security risks. The risks associated with outsourcing must be managed through the imposition of suitable controls, comprising a combination of legal, physical, logical, procedural and managerial controls.

3.23 Business continuity management

It is the policy of [REDACTED] to ensure that a Business Continuity Plan (including a DR Plan) are developed and tested in order to maintain the viability of the enterprise.

3.24 Change management

The Change management process must be followed to ensure all planned and unplanned changes to [REDACTED] operational services environment by internal or external (third party) resources.

3.25 Compliance

It is the policy of [REDACTED] to ensure that the IT infrastructure is in compliance with all legal, statutory, regulatory, and contractual requirements.

Compliance with the following rules is required:

- a) You may only use software that has been installed by an administrator.
- b) You shall not use a modem, dongle or any other devices to connect your computer to other networks and services, including the Internet, without authorization.
- c) Your password must be a minimum of 8 characters and it should be in accordance with the standard password criteria defined in the password management procedure.

Verify Version Before Use

Copyright © [REDACTED] All rights reserved. Unauthorized copy or use of this document is strictly prohibited

		Version: 1.1 RESTRICTED
<u>INFORMATION SECURITY POLICY DOCUMENT</u>		

- d) You shall not give your password to anybody else nor may you try to discover another person's password.
- e) You shall not disable Security features such as anti-virus or screen savers without authorization from administrator.
- f) You shall not allow strangers to work on your computer.
- g) You shall not give [REDACTED] information to other people.
- h) You shall not relocate your computer without informing line manager.
- i) You shall not knowingly introduce a computer virus into [REDACTED] computers.
- j) You shall not load media of unknown origin into the [REDACTED] computers. Incoming storage media must be scanned for viruses before they are read. If you suspect that your workstation has been infected by a virus, you must immediately power off the workstation and contact the Service Desk.
- k) You shall not download or send any material that is profane, indecent, subversive, and criminal or may contribute to harming others.
- l) You shall not use the WWW to access Internet Relay Chat rooms or news grouping without permission of CISO or his authorized representative.
- m) You shall not disclose information about the [REDACTED] its business or its customers and staff without the written authorization from [REDACTED] Management.
- n) You shall not waste IT resource of [REDACTED] by using them in unofficial activities. The use [REDACTED] resource to play games or at any time is strictly prohibited.

3.26 Internal Audit

Information Security department will conduct internal audit once in a year to ensure that the company continually operates in accordance with the specified policies, procedures and external requirements in meeting company goals and objectives.

3.27 Monitoring Usage

- a) At any time and without prior warning, the [REDACTED] may choose to examine e-mail messages, files, web browser bookmarks and other information on its computers.
- b) The [REDACTED] records this information to allow it to monitor its policies, to assist with internal investigations and to manage its IT systems. It is a condition of use that you accept that this may happen.

3.28 Information Security Services

shall implement following information security services across organization (subject to Risk Assessment)

- Access Control
- User Authentication (By users and programs)
- Message Authentication (Integrity)
- Privacy (Confidentiality)
- Non Repudiation (Responsibility)
- Availability

3.29 All activities on Information Systems are constantly monitored

- a) shall maintain the logs of Information Systems wherever required.
- b) The may require the completion of this form by business partners who are responsible for processing of information or maintenance of facilities for the processing of information on behalf of the
- c) Please ensure that you have read and understood the contents of this Information Security Statement of Awareness and Compliances and then complete and return this form to the HR department.

3.30 Sub Policies

shall maintain following sub-policies:

3.30.1 Acceptable Asset use policy

No one is permitted to use assets in a way that is:

- Damaging for the asset
- Not according to vendor's manual
- Not according to recognized best practices

3.30.2 Network Acceptable Use Policy

This Acceptable Use Policy is intended to communicate those actions that are considered inappropriate by to employees and people, who use public network and Internet for business and at home to facilitate the privacy, integrity and security of the systems, data, services, products and hosting facilities. The policy applies to all personnel, employees of

Verify Version Before Use

Copyright © All rights reserved. Unauthorized copy or use of this document is strictly prohibited

		Version: 1.1 RESTRICTED
<u>INFORMATION SECURITY POLICY DOCUMENT</u>		

the [REDACTED] at all levels of seniority. It applies to all of its facilities which are owned, leased or hired by [REDACTED] and all IT facilities used by staff either at [REDACTED] premises, or connected to [REDACTED] networks and all IT enabled communications (ISPs) entered into on behalf of the [REDACTED]

3.30.3 Software Usage Policy

Any operating system and software should be verified prior to install if it's the part of the software list that is approved by CISO. List will be available on portal and SAN. If not in approved, an application will be submitted to Information Security Committee to get it approved.

Only O&M designated personals are allowed to download any type of software. Before downloading it'll be verified if the right source is selected and in case of mirrors only certified mirror is selected to download the package. IF available, HASH will be verified after downloading the package.

If the newly download software is not freeware then it will be passed to corporate department for its licensing. In case of existing softwares the license will be verified from Information Security Committee to maintain its count and limit.

Only Information Security Committee's recommended path/place is valid for distribution of the softwares. Personally no one is allowed to distribute and get the softwares. Approved softwares have been defined within the Approved Software List document.

All the software is allowed for business purposes only, without CISO's approval no one is allowed to install any software on their personal and home PCs.

Information Security Analyst will be responsible for the licence expiry, renewals, counting and their security as well.

3.30.4 E-MAIL Policy

Management and staff must use the security features provided by the [REDACTED] standard e-mail system, such as digital signatures and read receipts, to confirm correct receipt of important internal e-mail messages when appropriate. In particular the encryption option must be used to protect confidential information within internal e-mails where appropriate (specifically for higher management). All users of external e-mail must be made aware that the Internet operates in the public domain outside of [REDACTED] control. Messages might be subject to delay and potentially unreliable services, and might be stored temporarily in insecure locations during transit. These factors are beyond [REDACTED] control. Management must therefore consider:

a) The need to encrypt the content of emails and attachments wherever justified by the business risks to information confidentiality.

Verify Version Before Use

Copyright © [REDACTED] All rights reserved. Unauthorized copy or use of this document is strictly prohibited

		Version: 1.1 RESTRICTED
<u>INFORMATION SECURITY POLICY DOCUMENT</u>		

b) The risks of delay to time critical messages. Additional procedural checks must be put in place to verify the arrival of the message. Where possible, 'receipt' and 'read' notifications must be requested.

c) The risks of breaches of confidentiality and social engineering from the use of facilities such as "out of office" messages and auto-forwarding of e-mail to addresses external to the [REDACTED] and similar facilities.

d) The business need for effective message logs and audit trails of message system use, particularly to satisfy regulatory requirements where relevant.



Email ID creation for [REDACTED] Employees will follow the standard procedures of First Name of the employees then ". "i.e. full stop followed by second name of employee e.g. [REDACTED] and if there are new employees whose names are similar to the old employees then the mail id will be with a number e.g. [REDACTED] In special cases, different nomenclature can however be followed.

When sending e-mail you must not:

- a) Use false identities.
- b) Send confidential information without seeking advice from the Information security committee.
- c) Create or forward advertisements or chain mails.

4 Enforcement

Enforcement of this policy is the responsibility of the Chief Information Security Officer within the framework of the [REDACTED] Information Security Management System Policies, procedures, and standards exist in support of this Information Security Management System. It is the responsibility of the Chief Information Security Officer to maintain and update the Information Security Management System as well as provide guidance for its implementation.

		Version: 1.1  RESTRICTED
<u>INFORMATION SECURITY POLICY DOCUMENT</u>		

5 Information Security Declaration

I declare that I have read understood and agree to abide by the Information Security Policy.

First Name: _____

Last Name: _____

Title: _____

Employee Number: _____

Department: _____

Section: _____

Signed: _____

Date: _____

( Employee Only)

Verify Version Before Use

Copyright ©   All rights reserved. Unauthorized copy or use of this document is strictly prohibited