CYBER SECURITY POLICY

FOOD CORPORATION OF INDIA

July 2014

FOREWORD

I am extremely happy that the IT Division of FCI has formulated the Cyber Security Policy for Food Corporation of India (FCI). I am sure that this effort will be a major step towards establishing secure ICT networks & Systems in FCI which will subsequently go a long way in streamlining the functions of the Corporation. This development is a move in the right direction enabling the Corporation to fulfill the mammoth task of ensuring Food Security of the Nation.

I congratulate our IT team in particular, and other divisions in general, for their untiring efforts in making the initiative a success within the stipulated time frame. I also thank Centre for Distributed Computing - Jadavpur University, Kolkata for their assistance in finalizing the Cyber Security Policy in a time bound manner.

I earnestly hope that this effort will be duly followed up by implementation of a full-fledged Information Security Management System in the Corporation in due course of time.

C.Viswanath
Chairman & Managing Director

Dated: 31.07.2014

PREFACE

In order to ensure a secure IT environment in FCI, it was decided by the Corporation to formulate the Cyber Security Policy document to protect the IT assets from various threats. Under the leadership and guidance of our Chairman and Managing Director, this activity was initiated in the month of May, 2014. Centre for Distributed Computing - Jadavpur University was engaged as a Consultant.

After the kick-off meeting on 3rd June, 2014, extensive discussions were held between the Consultant and all Divisions of FCI for eliciting the security requirements and Risk areas of FCI. Based on the requirements, the Scope of the Cyber Security Policy and Corporate Cyber Security Policy were developed. This was followed by the Security Baseline Categorization of FCI and identification of the Baseline Controls. Finally detailed Cyber Security Policies, Procedures, Guidelines and Forms were developed.

At each stage the IT Division team, other operating Divisions and Zonal & Region Heads were involved to review all the documents and provide feedbacks. All such feedbacks received were considered before finalizing the documents. I take this opportunity to thank all my colleagues for their keen interest and active participation in the entire exercise. Without their support, it would not have been possible to complete the task.

I firmly believe that enforcement of the Cyber Security Policy will help secure our systems and help all to adopt technology without any risks.

I am happy that we could fulfill the target within the time frame stipulated by the Memorandum of Understanding with Ministry.

Abhishek Singh
Executive Director (Information Technology)

Dated: 31.07.2014

Table of Contents

Revision History

Sl. No.	Date	Chapter No.	Revision No.	Change Summary

Chapter 1

Scope of Information Security Management System

Document Category: Cyber Security Policy

Document Classification: Internal

Access list: All employees of FCI

1. Purpose

In this document, the scope and boundaries for establishing, implementing, maintaining and continually improving the Information Security Management System (ISMS) of Food Corporation of India (FCI) are described. Organizational assets, including primary assets (Business Processes and Information) and supporting assets (Hardware, Software, Network, Personnel, Organizational Structure, and Site) are considered for defining ISMS scope.

2. Target Audience

The primary audiences for ISMS scope document are: Senior Management, System and Information Owners, Business and Functional Managers, Chief Information Security Officer (CISO), and IT Security Practitioners of the organization.

3. ISMS Scope and Boundaries

All IT-enabled Business Processes of FCI, namely Procurement, Storage, Movement & Distribution are included within the scope of ISMS. The scope also includes all critical and sensitive Information Assets of FCI, including paper documents.

All IT-enabled processes, currently being used at FCI, are covered within the scope of ISMS. This includes:

a. Integrated Information System for Food-grains Management (IISFM) which consists of District Information System for Food-grains Management (DISFM), IISFM Rapid Reporting Service (IRRS), and Depot Code Management System (DCMS);
b. E-tendering / E-Publishing;
c. Financial Accounting Package (FAP);
d. Human Resource Management System (HRMS);
e. E-litigation;
f. Procurement Monitoring System (PMS);
g. Release Order (RO) Module;
h. WINGS;
i. Movement Monitoring System;
j. Vigilance Complaint Monitoring System (VCMS).

The following applications, to be developed in the near future, are also covered within the scope of ISMS:

a. Engineering Works Management System (EWMS), for monitoring of all major engineering construction and maintenance activities in India; and
b. Godown Heath Management System (GHMS), for monitoring the conditions of godowns and action taken for replacement of major components, and review of regular maintenance including weighbridges as well as Memorandum of Understanding (MoU) targets.

The scope covers Employees, Contractors, and Third Party Employees, who may be bound by contractual agreements. Hardware assets, Software assets, Network assets, and Utilities, including Air Conditioner, Power and Telecommunication services, are the identified resources within the scope; equipment owned by third parties, but in the custody of FCI, will also be covered under the scope.

The entire organizational Intranet is within the scope of ISMS.

This ISMS will be applicable to all offices and facilities of FCI, including headquarters, zonal, regional, and district offices, and depots and purchase centres (if any IT facility exists in those centres). The facilities to be developed under future expansion plans, including software and other IT Systems, will automatically be included within the purview of ISMS.

4. Glossary

4.1 Asset - Anything that has value to the organization.

4.2 ISMS - Information Security Management System is the part of overall management system and required to establish, implement, maintain and continually improve information security of the organization.

Chapter 2

Corporate Policy for
Information Security Management System

Document Category: Cyber Security Policy

Document Classification: Public

Access list: All employees of FCI and other interested parties

1. Purpose

The purpose of Information Security Management System (ISMS) in Food Corporation of India (FCI) is to ensure the continuity and protection of the business processes and information assets which are considered within the ISMS scope (stated in ISMS scope document). The information security needs and objectives are stated in this document to minimize the impact of security incidents on the operations of FCI.

2. Target Audience

The primary audiences for Corporate Information Security Policy are: Senior Management, System and Information Owners, Business and Functional Managers, Chief Information Security Officer (CISO), and IT Security Practitioners of the organization.

3. Corporate ISMS Policy

The Information Security Management System of FCI intends to ensure:

3.1 Integrity of all business processes, information assets, and supporting IT assets and processes, through protection from unauthorized modification, guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. The unauthorized modification or destruction of information could have severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals;

3.2 Availability of all business processes, information assets, and supporting IT assets and processes to authorized users when needed, ensuring timely and reliable access to and use of information. The disruption of access to, or use of, information or an information system could have serious adverse effect on organizational operations, organizational assets, or individuals;

3.3 Confidentiality of all information assets (information is not disclosed to unauthorized persons through deliberate or careless action). Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. The unauthorized disclosure of information could have limited adverse effect on organizational operations, organizational assets, or individuals;

3.4 All IT-enabled processes and stakeholders shall follow the rules and regulations or circulars published in the organization;

3.5 All audit trails and logs, as decided by the Management Information Security Forum (MISF), shall be maintained and monitored by FCI;

3.6 All operational and system changes shall be monitored closely; these shall adhere to the change management process;

3.7 FCI complies with the laws, regulations and contractual obligations which are applicable to the organization in general and in particular to its ISMS;

3.8 All applicable information security requirements are satisfied;

3.9 Continual improvement of the information security management system.

4. Applicability

This policy applies to all officers and staff of FCI, contractors, and third party employees under contract, who have any access to, or involvement with, the business processes, information assets, and supporting IT assets and processes covered under the scope of ISMS.

5. Responsibility

FCI management shall ensure that all activities required to implement, maintain and review this policy are performed. All personnel, regarded as included in the ISMS scope, must comply with this policy statement and its related security responsibilities defined in the information security policies and procedures that support the corporate information security policy.

All personnel, even if not included in the ISMS scope, have a responsibility for reporting security incidents and identified weaknesses, and to contribute to the protection of business processes, information assets, and resources of FCI.

6. Enforcement

FCI holds the right to monitor the compliance of its personnel to this policy. Officers and staff of FCI, contractors, and third party employees, who fail to comply with this policy, may be subjected to appropriate disciplinary actions.

7. Ownership and Revision

This policy statement is owned by the Board of Directors of FCI who has delegated this task to the Chief Information Security Officer (CISO).

This policy shall be revised once in two years by the CISO and every time that the Board of Directors of FCI, or the MISF, decides to do so.

MISF of FCI shall consist of the following members (as approved by C&MD):
Executive Director (IT), Executive Director (Personnel), Executive Director (Finance), Executive Director (P&R) and Executive Director (Legal).

8. Glossary

8.1 Availability - Property of being accessible and usable upon demand by an authorized entity.

8.2 Asset - Anything that has value to the organization.

8.3 Confidentiality - Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

8.4 Integrity - Property of accuracy and completeness.

8.5 ISMS - Information Security Management System is the part of overall management system and required to establish, implement, maintain and continually improve information security of the organization.

Chapter 3

Information Classification and Handling Policy

Document Category: Cyber Security Policy

Document Classification: Internal

Access list: All employees of FCI

3.1 Mission Statement

To meet the enterprise business objectives and ensure continuity of its operations, FCI shall adopt and follow well-defined and time-tested plans and procedures, to ensure that sensitive information is classified correctly and handled as per organizational policies.

3.2 Introduction

Information is considered as primary asset of an organization. An organization uses different types of information assets. The sensitivity of these information assets may vary and similarly, their handling mechanisms are also different.

3.3 Purpose

The purpose of this policy is to ensure personal information and confidential information is protected from unauthorized use and disclosure. This policy helps to facilitate the identification of information to support routine disclosure and active dissemination of information. It also helps to protect the intellectual property of FCI.

3.4 Scope

3.4.1 Employees

This policy applies to all permanent employees, contractors, and third party employees who have access to IT assets of FCI and may be bound by contractual agreements.

3.4.2 IT Assets

This policy applies to all information assets of FCI.

3.4.3 Documentation

The policy documentation shall consist of Information Classification and Handling Policy and related procedures & guidelines.

3.4.4 Document Control

The Information Classification and Handling Policy document and all other referenced documents shall be controlled. Version control shall be to preserve the latest release and the previous version of any document. However, the previous version of the documents shall be retained only for a period of two years for legal and knowledge preservation purpose.

3.4.5 Records

Records being generated as part of the Information Classification and Handling Policy shall be retained for a period of two years. Records shall be in hard copy or electronic media. The records shall be owned by the respective system administrators and shall be audited once a year.

3.4.6 Distribution and Maintenance

The Information Classification and Handling Policy document shall be made available to all the employees covered in the scope. All the changes and new releases of this document shall be made available to the persons concerned. The maintenance responsibility of this document shall be with the CISO and website administrator.

3.5 Privacy

The Information Classification and Handling Policy document shall be considered as "confidential" and shall be made available to the concerned persons with proper access control. Subsequent changes and versions of this document shall be controlled.

3.6 Responsibility

The CISO / designated personnel is responsible for proper implementation of the Information Classification and Handling Policy.

3.7 Policy

FCI categorizes information into four classes: Confidential, Project / Process / Department specific, Internal, and Public.

a. **Confidential -** The information assets which have high confidentiality value belong to this category. Only a limited set of authorized users shall access these information assets. Examples include business strategy and personnel files.

b. **Project / Process / Department specific -** The information assets that contain data pertaining to the needs of a specific department, project team, or business process, belong to this category. Such information assets shall be accessible to members of the concerned department, project, or business process only.

c. **Internal -** The information assets which can be distributed within all offices of FCI belong to this category. Examples are office orders and internal circulars.

d. **Public -** The information assets which do not have any confidentiality requirement and / or can be disseminated to the general public belong to this category. Examples include annual financial report of FCI and information displayed on FCI's website.

Following are the policies for secure handling of information assets of FCI:

a. Handling and labeling of all media shall be according to its indicated classification level.

b. Depending on the classification of information, electronic transmission, copying and distribution of copies of such information, shall require prior approval of CISO / DGM / GM / ED / CMD, as applicable.

c. Mailing and/or shipment of confidential information shall require that information be sent through a reputed mail service / courier with proper authentication.

d. Confidential information shall be stored with proper security and / or in safe lockers.

e. Disposition of confidential and Project / Process / Department specific information shall require shredding in the presence of CISO / DGM / GM / ED / CMD / Process In-charge, as applicable.

f. Appropriate access restrictions shall be applied to prevent access from unauthorized personnel.

g. Formal record of the authorized recipients of data shall be maintained.

h. Information processing operations shall ensure the following: that input data is complete, that processing is properly completed, and that output validation is applied.

i. Storage of media shall be in accordance with the manufacturers' specifications.

j. All copies of media shall be clearly marked for the attention of the authorized recipient.

k. Spooled data awaiting output shall be protected to a level consistent with its sensitivity.

l. Distribution of data shall be based on "need to know" and "need to use" principles.

m. Distribution lists and lists of authorized recipients shall be reviewed at regular intervals.

3.8 Enforcement

Any employee found to have violated this policy may be subjected to disciplinary action in line with the HR Policy / Staff Regulation Act of FCI.

Chapter 4

Acceptable Use Policy

Document Category: Cyber Security Policy

Document Classification: Internal

Access list: All employees of FCI

4.1 Mission Statement

To meet the enterprise business objectives and ensure acceptable use of its information systems and networks, FCI shall adopt and follow well-defined and time-tested plans and procedures, and follow guidelines to exercise judgement regarding use of organizational resources.

4.2 Introduction

FCI is deploying IT-enabled services at various internal divisions for managing its business activities.

Presently FCI depends on the following IT-enabled processes for managing its business activities:

a. Integrated Information System for Food-grains Management (IISFM) which consists of District Information System for Food-grains Management (DISFM), IISFM Rapid Reporting Service (IRRS), and Depot Code Management System (DCMS);
b. E-tendering / E-Publishing;
c. Financial Accounting Package (FAP);
d. E-litigation;
e. Procurement Monitoring System (PMS);
f. Release Order (RO) Module.

The following processes are in conceptualization / development stage will be implemented in future:

a. Human Resource Management System (HRMS);
b. WINGS;
c. Movement Monitoring System;
d. Vigilance Complaint Monitoring System (VCMS).

The acceptable use policy and guidelines shall be communicated to and understood by all the employees of FCI.

The acceptable use policy and guidelines shall be available to the CMD, all EDs, GMs, DGMs, AGMs, managers, and CISO of FCI.

4.3 Purpose

The purpose of this policy is to outline the acceptable use of IT assets at FCI. These rules are in place to protect the employees and the organization. Inappropriate use exposes FCI to risks including virus attacks, compromise of network systems and services, and legal issues.

4.4 Scope

4.4.1 Employees

This policy applies to all FCI Employees, Contractors, and Third Party Employees, who have access to IT assets of FCI and may be bound by contractual agreements.

4.4.2 IT Assets

The policy is applicable to all Hardware assets, Software assets, Network assets, and Utilities, including Air Conditioner, Power and Telecommunication services (that serve IT assets of FCI). Equipment owned by third parties, but in the custody of FCI, will also be covered under the scope.

4.4.3 Documentation

The documentation shall consist of Acceptable Use Policy, guidelines and policies & procedures for acceptable use of each service.

4.4.4 Document Control

The Acceptable Use Policy document and all other referenced documents shall be controlled. Version control shall be to preserve the latest release and the previous version of any document. However, the previous version of the documents shall be retained only for a period of two years for legal and knowledge preservation purpose.

4.4.5 Records

Records being generated as part of the Acceptable Use Policy shall be retained for a period of two years. Records shall be in hard copy or electronic media. The records shall be owned by the respective system administrators and shall be audited once a year.

4.4.6 Distribution and Maintenance

The Acceptable Use Policy document shall be made available to all the employees covered in the scope. All the changes and new releases of this document shall be made available to the persons concerned. The maintenance responsibility of the document shall be with the CISO and system administrators.

4.5 Privacy

The Acceptable Use Policy document shall be considered as "confidential" and shall be made available to the concerned persons with proper access control. Subsequent changes and versions of this document shall be controlled.

4.6 Responsibility

The Acceptable Use Policy shall be implemented by the CISO / designated personnel.

4.7 Policy

4.7.1 General Use and Ownership

a. While the security administration of FCI desires to provide a reasonable level of privacy, users should be aware that the data they create on corporate systems remains the property of FCI. Because of the need to protect the IT assets of FCI, management cannot guarantee the confidentiality of personal information stored on any IT asset belonging to FCI.

b. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet and Intranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

c. It is recommended that any information that users consider sensitive or vulnerable be protected. For guidelines on information classification, refer "Information classification and handling policy".

d. For IT system security and network maintenance purposes, authorized individuals within FCI shall monitor equipment, systems and network traffic at any time, as per its IT Audit Policy or orders issued by the competent authority.

e. FCI reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.7.2 Security and Proprietary Information

a. The user interface for information contained on Internet and Intranet-related systems shall be classified accordingly. Employees shall take all necessary steps to prevent unauthorized access to this information.

b. Authorized users shall be responsible for the security of their passwords and accounts.

c. Encryption of information, if used, shall be in compliance with FCI's Cryptographic Control Usage Policy.

d. Information contained on portable computers shall be protected.

e. Users and employees shall use suitable procedures and guidelines for acceptable use of E-mail and internet resources.

4.7.3 Unacceptable Use

Under no circumstances is an employee of FCI authorized to engage in any activity that is illegal under national or international law while utilizing FCI-owned resources. The guidelines for Acceptable Use can be referred for a list of activities which fall under the category of unacceptable use.

4.8 Enforcement

Any employee found to have violated this policy may be subjected to disciplinary action in line with the HR Policy / Staff Regulation Act of FCI.

Chapter 5

Access Control Policy

Document Category: Cyber Security Policy

Document Classification: Internal

Access list: All employees of FCI

5.1 Mission Statement

To meet the enterprise business objectives and ensure continuity of its operations, FCI shall adopt and follow well-defined and time-tested plans and procedures, to control access to organizational network and information system resources by identifying and managing access of employees, contractors, third party employees, guests, and non-compliant IT systems.

5.2 Introduction

Access to IT resources is critical for FCI employees, contractors, and third party employees to effectively perform their job duties. Securing and protecting organizational IT resources is a critical responsibility of every individual with access to FCI IT resources. Failure to be vigilant by any one individual may put everyone at risk.

The policy, and respective procedures, guidelines and forms such as "Facilities allocation forms" shall be available to the CMD, all EDs, GMs, DGMs, AGMs, managers, and CISO of FCI.

5.3 Purpose

The purpose of this policy is to control access to the organizational IT assets.

5.4 Scope

5.4.1 IT Assets

This policy applies to all organizational employees, contractors, third party employees, and vendors with access to organizational IT resources. The policy applies to all access into the FCI network or any system owned, leased, or supported by FCI that stores protected organizational information.

5.4.2 Documentation

The documentation shall consist of Access Control Policy and various access control guidelines for each IT-enabled process of FCI.

5.4.3 Document Control

The Access Control Policy document and all other referenced documents shall be controlled. Version control shall be used to preserve the latest release and the previous version of any document.

However, the previous version of the documents shall be retained only for a period of two years for legal and knowledge preservation purpose.

5.4.4 Records

Records being generated as part of the Access Control Policy shall be retained for a period of two years. Records shall be in hard copy or electronic media. The records shall be owned by the respective system administrators and shall be audited once a year.

5.4.5 Distribution and Maintenance

The Access Control Policy document shall be made available to all the employees covered in the scope. All the changes and new releases of this document shall be made available to the persons concerned. The maintenance responsibility of the document shall be with the CISO and system administrators.

5.5 Privacy

The Access Control Policy document shall be considered as "confidential" and shall be made available to the concerned persons with proper access control. Subsequent changes and versions of this document shall be controlled.

5.6 Responsibility

The CISO / designated personnel is responsible for proper implementation of the Access Control Policy.

5.7 Policy

Access to IT assets shall be given to users considering the following parameters:

a. Security requirements of individual business applications;

b. Identification of all information relating to business applications;

c. Information dissemination and authorization, i.e., the need to know principle and security levels and reference to guidelines relating to classification of information;

d. Consistency between the access control and information classification policies of different IT systems and networks;

e. Relevant legislation and any contractual obligation regarding protection of access to data or services;

f. Standard user access profiles for common categories of jobs;

g. Management of access rights in a distributed and networked environment, which recognizes all types of connections available;

h. Controlled access for both internal and external networked services;

i. Distinction between rules that must always be enforced and those, which are optional, shall be done; special rules allow users to override system controls;

j. Establishing rules based on the premise "what must be generally forbidden unless expressly permitted" rather than the weaker rule that "everything is generally permitted unless expressly forbidden";

k. Changes in information labels that are initiated automatically by information processing facilities and those initiated at the discretion of the user;

l. Changes in user permission that are initiated automatically by the information system and those initiated by the administrator;

m. Rules, which require administrator or other approval before enforcement and those, which do not.

5.8 Enforcement

Any employee found to have violated this policy may be subjected to disciplinary action in line with the HR Policy / Staff Regulation Act of FCI.

Chapter 6

Media Handling Policy

Document Category: Cyber Security Policy

Document Classification: Internal

Access list: All employees of FCI

6.1 Mission Statement

To meet the enterprise business objectives and ensure acceptable use of its information systems and networks, FCI shall adopt and follow well-defined and time-tested plans and procedures, follow guidelines to ensure secure management of media to protect sensitive or personal information from intentional or accidental exposure or misuse.

6.2 Introduction

Media is anything on which information or data can be recorded or stored and includes both paper and a variety of electronic media. Storage devices include but are not limited to: computer hard drives, portable hard drives, backup tapes, DVD / CD media, USB drives and other Personal Digital Assistants (PDA), cell phones, iPods, MP3 players, digital cameras, fax machines, and photocopiers. When handling and managing information it is essential to understand that maintaining security for both the information and the media on which it is stored is equally important.

6.3 Purpose

This Policy offers guidance regarding media handling. It is intended to guide and inform personnel and help them understand their roles and responsibilities according to the policy.

6.4 Scope

6.4.1 Employees

This policy applies to all FCI Employees, Contractors, and Third Party Employees, who use media of FCI.

6.4.2 IT Assets

This policy applies to all organizational IT assets of FCI.

6.4.3 Documentation

The documentation shall consist of Media Handling Policy, and related procedures & guidelines.

6.4.4 Document Control

The Media Handling Policy document and all other referenced documents shall be controlled. Version control shall be to preserve the latest release and the previous version of any document. However, the previous version of the documents shall be retained only for a period of two years for legal and knowledge preservation purpose.

6.4.5 Records

Records being generated as part of the Media Handling Policy shall be retained for a period of two years. Records shall be in hard copy or electronic media. The records shall be owned by the respective system administrators and shall be audited once a year.

6.4.6 Distribution and Maintenance

The Media Handling Policy document shall be made available to all the employees covered in the scope. All the changes and new releases of this document shall be made available to the persons concerned. The maintenance responsibility of the document shall be with the CISO and system administrators.

6.5 Privacy

The Media Handling Policy document shall be considered as "confidential" and shall be made available to the concerned persons with proper access control. Subsequent changes and versions of this document shall be controlled.

6.6 Responsibility

The Media Handling Policy shall be implemented by the CISO / designated personnel.

6.7 Policy

The primary area of concern is secure management of media to protect sensitive or personal information from intentional or accidental exposure or misuse. The following shall be implemented:

a. Risks to information and the media on which it resides shall be securely managed throughout the lifecycle of procurement, use, storage and disposition.

b. Only government authorized media shall be used for managing data.

c. Erasure of information from media shall be done by approved standards and secure disposal of media shall be followed using documented procedures.

d. Media shall be handled according to the highest level of sensitivity of contained information.

e. Media shall be protected from theft or tampering.

f. Where there is re-assignment or destruction of hardware and media, inventory records shall be kept current.

6.8 Enforcement

Any employee found to have violated this policy may be subjected to disciplinary action in line with the HR Policy / Staff Regulation Act of FCI.

Chapter 7

Password Policy

Document Category: Cyber Security Policy

Document Classification: Internal

Access list: All employees of FCI

7.1 Mission Statement

It is imperative that users practice due diligence in controlling access to their systems by protecting their user accounts with passwords which are not easily guessed or deduced.

7.2 Introduction

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the entire corporate network of FCI. As such, all FCI employees (including contractors and vendors with access to systems of FCI) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

7.3 Purpose

The purpose of this policy is to ensure that secure practices are introduced and maintained by all employees of FCI with respect to password protected information infrastructure.

7.4 Scope

7.4.1 IT Assets

The policy is applicable for all IT systems and services.

7.4.2 Documentation

The documentation shall consist of Password Policy and related guidelines.

7.4.3 Document Control

The Password Policy document and all other referenced documents shall be controlled. Version control shall be to preserve the latest release and the previous version of any document. However, the previous version of the documents shall be retained only for a period of two years for legal and knowledge preservation purpose.

7.4.4 Records

Records being generated as part of the Password Policy shall be retained for a period of two years. Records shall be in hard copy or electronic media. The records shall be owned by the respective system administrators and shall be audited once a year.

7.4.5 Distributions and Maintenance

The Password Policy document shall be made available to all the employees covered in the scope. All the changes and new releases of this document shall be made available to the persons concerned. The maintenance responsibility of the document will be with the CISO and system administrators.

7.5 Privacy

The Password Policy document shall be considered as "confidential" and shall be made available to the concerned persons with proper access control. Subsequent changes and versions of this document shall be controlled.

7.6 Responsibility

The Password Policy shall be implemented by the CISO / designated personnel.

7.7 Policy

a. Password policy shall ensure that all user accounts are protected by strong passwords and that the strength of the passwords meets the security requirements of the system.

b. The concept of ageing shall be used for passwords. Passwords on their expiry shall cease to function.

c. Users shall be educated about password protection and the password policy shall be implemented to ensure that users follow best practices for password protection.

d. IT systems shall be configured to prevent password reuse.

e. For critical information systems, account lockout strategy shall be defined. This shall be based on a risk analysis of the system as well as the costs to be incurred in case such strategy is implemented.

f. Standards such as LDAP (Internet) and X.500 (ITU-T/ISO) shall be referred for standardizing secure password practices.

7.8 Enforcement

Any employee found to have violated this policy may be subjected to disciplinary action in line with the HR Policy / Staff Regulation Act of FCI.

Chapter 8

E-mail Policy

Document Category: Cyber Security Policy

Document Classification: Internal

Access list: All employee of FCI

8.1 Mission Statement

The E-mail policy helps prevent tarnishing the public image of FCI. When E-mail goes out from FCI, the general public will tend to view that message as an official statement from the organization.

8.2 Introduction

FCI provides electronic mail to staff to enable them to communicate effectively and efficiently with other members of staff, other companies and partner organizations. When using the Organization's electronic mail facilities all employees shall comply with the email policy.

8.3 Purpose

The purpose of this policy is to reduce security risks created in the organization due to use of electronic mail.

8.4 Scope

8.4.1 IT Assets

This policy applies to all information systems and employees of FCI.

8.4.2 Documentation

The documentation shall consist of E-mail Policy, and related procedures and guidelines.

8.4.3 Document Control

The E-mail Policy document and all other referenced documents shall be controlled. Version control shall be to preserve the latest release and the previous version of any document. However, the previous version of the documents shall be retained only for a period of two years for legal and knowledge preservation purpose.

8.4.4 Records

Records being generated as part of the E-mail Policy shall be retained for a period of two years. Records shall be in hard copy or electronic media. The records shall be owned by the respective system administrators and shall be audited once a year.

8.4.5 Distribution and Maintenance

The E-mail Policy document shall be made available to all the employees covered in the scope. All the changes and new releases of this document shall be made available to the persons concerned. The maintenance responsibility of the document shall be with the CISO and system administrators.

8.5 Privacy

The E-mail Policy document shall be considered as "confidential" and shall be made available to the concerned persons with proper access control. Subsequent changes and versions of this document shall be controlled.

8.6 Responsibility

The E-mail Policy shall be implemented by the CISO / designated personnel.

8.7 Policy

E-mail shall only be used for business purposes, using terms, which are consistent with other forms of business communication. E-mail guidelines are intended to help users make the best use of the electronic mail facilities at their disposal. When using the organization's electronic mail facilities, users should comply with the E-mail guidelines.

8.8 Enforcement

Any employee found to have violated this policy may be subjected to disciplinary action in line with the HR Policy / Staff Regulation Act of FCI.

Chapter 9

Clear Desk and Clear Screen Policy

Doc. No:

Document Category: Cyber Security Policy

Document Classification: Internal

Access list: All employee of FCI

9.1 Mission Statement

The Clear Desk and Clear Screen Policy shall communicate the Management's intent to protect information stored in physical and electronic media and minimize risk of unauthorized access.

9.2 Introduction

Information is an asset which, like other important business assets, has value to FCI and consequently needs to be suitably protected. Information, in whatever form it takes, or means by which it is shared or stored, should always be appropriately protected.

9.3 Purpose

To improve the security and confidentiality of information, wherever possible a clear desk policy for papers and removable storage media and clear screen policy for information processing facilities shall be adopted. This shall reduce the risk of unauthorized access, loss of, and damage to information during and outside normal working hours or when areas are unattended.

9.4 Scope

9.4.1 IT Assets

This policy applies to all FCI Employees, Contractors, and Third Party Employees, who have access to IT assets of FCI and may be bound by contractual agreements.

9.4.2 Documentation

The Policy documentation shall consist of Clear Desk and Clear Screen Policy and related guidelines.

9.4.3 Document Control

The Clear Desk and Clear Screen Policy document and all other referenced documents shall be controlled. Version control shall be to preserve the latest release and the previous version of any document. However, the previous version of the documents shall be retained only for a period of two years for legal and knowledge preservation purpose.

9.4.4 Records

Records being generated as part of the Clear Desk and Clear Screen Policy shall be retained for a period of two years. Records shall be in hard copy or electronic media. The records shall be owned by the respective system administrators and shall be audited once a year.

9.4.5 Distribution and Maintenance

The Clear Desk and Clear Screen Policy document shall be made available to all the employees covered in the scope. All the changes and new releases of this document shall be made available to the persons concerned. The maintenance responsibility of the Clear Desk and Clear Screen Policy document shall be with the CISO and system administrators.

9.5 Privacy

The Clear Desk and Clear Screen Policy document shall be considered as "confidential" and shall be made available to the concerned persons with proper access control. Subsequent changes and versions of this document shall be controlled.

9.6 Responsibility

The CISO / designated personnel is responsible for proper implementation of the Policy.

9.7 Policy

a. Computers / computer terminals shall not be left logged-on when unattended and shall be password-protected.

b. The Windows Security Lock shall be set to activate when there is no activity for three minutes.

c. The Windows Security Lock shall be password protected for reactivation.

d. Users shall shut down their machines when they leave for the day.

e. There shall be no screen savers set on for the individual's desktops and laptops.

f. Where practically possible, paper and computer media shall be stored in suitable locked safes, cabinets or other forms of security furniture when not in use, especially outside working hours.

g. Sensitive or classified information, when printed, shall be cleared from printers immediately.

h. The reception desk can be particularly vulnerable to visitors. This area shall be kept as clear as possible at all times.

i. Individual's belongings like bags, books, edibles etc. shall be kept in drawers.

j. Before leaving for the day an individual shall make sure not to leave any paper or belongings on the desk.

k. Desktops shall have only shortcuts instead of having complete files or folders.

l. Computer screens shall be angled away from the view of unauthorized persons.

m. Physical access to the information system device that displays information shall be controlled to prevent unauthorized individuals from observing the display output.

n. Server rooms and office areas shall remain locked when they are not in use.

9.8 Enforcement

Any employee found to have violated this policy may be subjected to disciplinary action in line with the HR Policy / Staff Regulation Act of FCI.

Chapter 10

Anti-Malware Policy

Document Category: Cyber Security Policy

Document Classification: Internal

Access list: All employees of FCI

10.1 Mission Statement

To meet the enterprise business objectives and ensure continuity of its operations, FCI shall adopt and follow well-defined and time-tested plans and procedures, to ensure protection of IT assets from malware and virus attacks.

10.2 Introduction

IT assets must be employed in ways that achieve the business objectives of FCI. IT assets shall be protected in a way that ensures that they are resistant to virus and malware attacks and that all preventive and protective measures shall be used to resist such malware attacks.

The policy, and respective procedures, guidelines and forms such as facilities allocation forms shall be available to the CMD, all EDs, GMs, DGMs, AGMs, managers, and CISO of FCI.

10.3 Purpose

The purpose of this policy is to promote the use of anti-virus and other anti-malware software and educate the employees of FCI regarding the policies that are widely followed to use an anti-malware effectively. Besides, this policy provides direction to ensure that legal regulations are followed.

10.4 Scope

10.4.1 Employees

This policy applies to all FCI Employees, Contractors, and Third Party Employees, who have access to IT assets of FCI and may be bound by contractual agreements.

10.4.2 IT Assets

This policy applies to all workstations and servers that are owned or leased by FCI.

10.4.3 Documentation

The Policy documentation shall consist of Anti-malware Policy and related guidelines.

10.4.4 Document Control

The Anti-Malware Policy document and all other referenced documents shall be controlled. Version control shall be used to preserve the latest release and the previous version of any document. However, the previous version of the documents shall be retained only for a period of two years for legal and knowledge preservation purpose.

10.4.5 Records

Records being generated as part of the Anti-Malware Policy shall be retained for a period of two years. Records shall be in hard copy or electronic media. The records shall be owned by the respective system administrators and shall be audited once a year.

10.4.6 Distribution and Maintenance

The Anti-Malware Policy document shall be made available to all the employees covered in the scope. All the changes and new releases of this document shall be made available to the persons concerned. The maintenance responsibility of the document shall be with the CISO and system administrators.

10.5 Privacy

The Anti-Malware Policy document shall be considered as "confidential" and shall be made available to the concerned persons with proper access control. Subsequent changes and versions of this document shall be controlled.

10.6 Responsibility

The CISO / designated personnel is responsible for proper implementation of the Policy.

10.7 Policy

FCI shall adopt certain practices to prevent malware problems:

i. All workstations whether connected to FCI network, or standalone, must use FCI-approved anti-virus and anti-malware software and configuration.

ii. The anti-virus and anti-malware software must not be disabled or bypassed.

iii. The settings for the anti-virus and anti-malware software must not be altered in a manner that will reduce the effectiveness of the software.

iv. The automatic update frequency of the anti-virus and anti-malware software must not be altered to reduce the frequency of updates.

v. Each file server attached to FCI network must utilize FCI-approved anti-virus and anti-malware software and setup to detect and clean malware that may infect file shares.

vi. Every virus / malware that is not automatically cleaned by the anti-virus and anti-malware software constitutes a security incident and must be reported to the Help Desk.

vii. The organization shall adopt suitable controls to prevent and detect the introduction of malicious code and unauthorized mobile code.

viii. The information system automatically updates malicious code protection mechanisms e.g. automatic updates of anti-virus and anti-malware software.

ix. Each E-mail gateway must utilize FCI-approved e-mail anti-virus software and must adhere to the ISMS rules for the setup and use of this software.

10.8 Enforcement

Any employee found to have violated this policy may be subjected to disciplinary action in line with the HR Policy / Staff Regulation Act of FCI.

Chapter 11

Cryptographic Control Usage Policy

Document Category: Cyber Security Policy

Document Classification: Internal

Access list: All employee of FCI

11.1 Mission Statement

The Cryptographic Control Usage Policy shall communicate the management's approach towards the use of cryptographic controls across FCI, including the general principles under which business information shall be protected.

11.2 Introduction

Information is an asset which, like other important business assets, has value to FCI and consequently needs to be suitably protected. Information, in whatever form it takes, or means by which it is shared or stored, should always be appropriately protected. Cryptographic techniques may be used to protect integrity and authenticity of information.

11.3 Purpose

The purpose of this policy is to ensure that benefits of using cryptographic controls are maximized and corresponding risks are minimized. The policy also ensures that inappropriate or incorrect use of cryptographic controls within FCI is avoided.

11.4 Scope

11.4.1 IT Assets

This policy applies to all organizational information systems within FCI.

11.4.2 Documentation

The Policy documentation shall consist of Cryptographic Control Usage Policy and related guidelines.

11.4.3 Document Control

The Cryptographic Control Usage Policy document and all other referenced documents shall be controlled. Version control shall be to preserve the latest release and the previous version of any document. However, the previous version of the documents shall be retained only for a period of two years for legal and knowledge preservation purpose.

11.4.4 Records

Records being generated as part of the Cryptographic Control Usage Policy shall be retained for a period of two years. Records shall be in hard copy or electronic media. The records shall be owned by the respective system administrators and shall be audited once a year.

11.4.5 Distribution and Maintenance

The Cryptographic Control Usage Policy document shall be made available to all the employees covered in the scope. All the changes and new releases of this document shall be made available to the persons concerned. The maintenance responsibility of the Cryptographic Control Usage Policy document shall be with the CISO and system administrators.

11.5 Privacy

The Cryptographic Control Usage Policy document shall be considered as "confidential" and shall be made available to the concerned persons with proper access control. Subsequent changes and versions of this document shall be controlled.

11.6 Responsibility

The CISO / designated personnel is responsible for proper implementation of the Policy.

11.7 Policy

The management approach towards the use of cryptographic controls across the organization, including the general principles under which business information must be protected, shall be fixed. The approach to key management, including methods to deal with the recovery of encrypted information in case of lost, compromised or damaged keys, shall be laid down appropriately. As for roles and responsibilities, the management of FCI shall designate person(s) for implementation of the policy.

11.8 Enforcement

Any employee found to have violated this policy may be subjected to disciplinary action in line with the HR Policy / Staff Regulation Act of FCI.

Chapter 12

Backup Policy

Document Category: Cyber Security Policy

Document Classification: Internal

Access list: All employees of FCI

12.1 Mission Statement

To meet the enterprise business objectives and ensure continuity of its operations, FCI shall adopt and follow well-defined and time-tested plans and procedures, to ensure timely and reliable backup of its IT assets.

12.2 Introduction

The Backup Policy reiterates the commitment of FCI towards delivering the fastest transition and highest quality of services through the backup arrangement ensuring that its customers, business activities and services do not suffer in any way.

The policy shall be available to the CISO and BCP (Business Continuity Plan) team members of FCI.

12.3 Purpose

The purpose of this policy is to provide means to:

i. restore the integrity of the computer systems in the event of a hardware/software failure or physical disaster; and
ii. provide a measure of protection against human error or the inadvertent deletion of important files.

12.4 Scope

12.4.1 Employees

This policy applies to all FCI Employees, Contractors, and Third Party Employees, who have access to IT assets of FCI and may be bound by contractual agreements.

12.4.2 IT Assets

This policy applies to the entire IT infrastructure of FCI.

12.4.3 Documentation

The Policy documentation shall consist of Backup Policy and related procedures and guidelines.

12.4.4 Document Control

The Backup Policy document and all other referenced documents shall be controlled. Version control shall be used to preserve the latest release and the previous version of any document. However, the previous version of the documents shall be retained only for a period of two years for legal and knowledge preservation purpose.

12.4.5 Records

Records being generated as part of the Backup Policy shall be retained for a period of two years. Records shall be in hard copy or electronic media. The records shall be owned by the respective system administrators and shall be audited once a year.

12.4.6 Distribution and Maintenance

The Backup Policy document shall be made available to all the employees covered in the scope. All the changes and new releases of this document shall be made available to the persons concerned. The maintenance responsibility of the document shall be with the CISO and system administrators.

12.5 Privacy

The Backup Policy document shall be considered as "confidential" and shall be made available to the concerned persons with proper access control. Subsequent changes and versions of this document shall be controlled.

12.6 Responsibility

The CISO / designated personnel is responsible for proper implementation of the Policy.

12.7 Policy

a. All user-level and system-level information maintained by FCI shall be backed up periodically. The backup media shall be stored with sufficient protection and proper environmental conditions. The systems backups shall be taken based on the schedule as outlined in the backup guidelines document. Alternatively, FCI shall be able to perform backup by customizing backup schedule according to the requirements of the organization. The backup guidelines can be used for reference in formulating FCI's backup schedule. Back-up schedule of servers maintained at NIC shall be drawn up in consultation with NIC.

b. To confirm media reliability and information integrity, the back-up information shall be tested at some specified frequency.

c. Backup information shall be selectively used to restore information system functions as a part of business continuity process.

d. Backup copies of operating systems and other critical information system software shall not be stored in the same location as the operational software.

e. The system backup information shall be provided with protection from unauthorized modification and environmental conditions.

12.8 Enforcement

Any employee found to have violated this policy may be subjected to disciplinary action in line with the HR Policy / Staff Regulation Act of FCI.

Chapter 13

Business Continuity Management Policy

Document Category: Cyber Security Policy

Document Classification: Internal

Access list: All employees of FCI

13.1 Mission Statement

To meet the enterprise business objectives and ensure continuity of its operations, FCI shall adopt and follow well-defined and time-tested plans and procedures, build redundancy in teams and infrastructure, and manage a quick and efficient transition to the backup arrangement for business systems and services.

13.2 Introduction

Business Continuity Management (BCM) Policy reiterates the commitment of FCI towards delivering the fastest transition and the highest quality of services through backup arrangement ensuring that the customers, business activities and services do not suffer in any way. The Business Continuity Management Procedure, Backup Policy and Backup Procedure shall be referred.

The plan shall be available to the CISO and BCM team members of FCI.

13.3 Purpose

The main objective of Business Continuity Management is to minimize / eliminate the loss to organization's business in terms of revenue loss, loss of reputation, loss of productivity and customer satisfaction. The Business Continuity Policy intends to:

a. establish a systematic approach for business continuity;
b. create awareness amongst the concerned employees, about the business continuity aspects of ISMS and its importance; and
c. test and review the business continuity plan for the organization.

13.4 Scope

13.4.1 IT Assets

BCM covers all IT assets and applications for business transaction that are owned or utilized by FCI.

13.4.2 Documentation

The BCM documentation shall consist of Plans and Resumption procedures for each service.

13.4.3 Document Control

The BCM document and all other referenced documents shall be controlled. The version control shall be used to preserve the latest release and the previous version of any document. However, the previous version of the documents shall be retained only for a period of two years for legal and knowledge preservation purpose.

13.4.4 Records

Records being generated as part of the BCM shall be retained for a period of two years. Records shall be in hard copy or electronic media. The records shall be owned by the respective system administrators and shall be audited once a year.

13.4.6 Distribution and Maintenance

The BCM document shall be made available to all the employees covered in the scope. All the changes and new releases of this document shall be made available to the persons concerned. The maintenance responsibility of the BCP document will be with the CISO and BCM team.

13.5 Privacy

The BCM document shall be considered as "confidential" and shall be made available to the concerned persons with proper access control. Subsequent changes and versions of this document shall be controlled.

13.6 Responsibility

Role of BCM Leader shall be performed by CISO and include the following:

a. Coordinate the development and maintenance of the Organizational BCM policy manual and get approval from MISF (Management Information Security Forum).
b. Identify and declare disaster-scenarios according to the gravity of the disaster.
c. Enforce BCM among teams as per disaster scenarios.
d. Review and audit BCM Policy at planned intervals.
e. Test and update Business Continuity Plan at planned intervals.
f. Facilitate functional training of the members for BCM execution.
g. Co-ordinate with outsourcing partners wherever applicable.

Following are the primary roles of BCM Team Members:

a. Execute BCM activities as per respective procedures.
b. Co-ordinate with outsourcing partners wherever applicable.

13.7 Policy

a. For **catastrophic** and **major** disasters, the BCM Leader shall invoke the BCM process in consultation with the BCM Team Members.

b. It is the responsibility of the BCM Leader to ensure that adequate spare resources are available for recovering from disaster in the infrastructure level.

c. It is mandatory for all BCM Team Leaders to maintain the BCM document in an easily accessible and secure location.

d. The BCM Policy shall be updated whenever major additions, upgrades, deletions take place to the underlying hardware, network environment, office infrastructure or key personnel.

e. The BCM Policy and Plan testing process for vital services shall be done at least once in a year.

13.8 Enforcement

Any employee found to have violated this policy may be subjected to disciplinary action in line with the HR Policy / Staff Regulation Act of FCI.

Chapter 14

Disaster Recovery Policy

Document Category: Cyber Security Policy

Document Classification: Internal

Access list: All employee of FCI

14.1 Mission Statement

To meet the enterprise business objectives, respond to a major incident or disaster, and restore the organization's critical business functions, FCI shall adopt and follow well-defined and time-tested plans and procedures.

14.2 Introduction

Disaster recovery policy is required to respond to a major incident or disaster by implementing a plan to restore FCI's critical business functions.

14.3 Purpose

The purpose of this policy is to ensure that IT resource investments made by FCI are protected against service interruptions, including large scale disasters, by the development, implementation, and testing of disaster recovery / business continuity plans (DR/BCP).

14.4 Scope

14.4.1 IT Assets

This policy applies to all facilities of FCI that operate, manage, or use IT services or equipment to support critical business functions.

14.4.2 Documentation

The documentation shall consist of Disaster Recovery Policy, and related procedures and guidelines.

14.4.3 Document Control

The Disaster Recovery Policy document and all other referenced documents shall be controlled. Version control shall be to preserve the latest release and the previous version of any document. However, the previous version of the documents shall be retained only for a period of two years for legal and knowledge preservation purpose.

14.4.4 Records

Records being generated as part of the Disaster Recovery Policy shall be retained for a period of two years. Records shall be in hard copy or electronic media. The records shall be owned by the respective system administrators and shall be audited once a year.

14.4.5 Distribution and Maintenance

The Disaster Recovery Policy document shall be made available to all the employees covered in the scope. All the changes and new releases of this document shall be made available to the persons concerned. The maintenance responsibility of the document shall be with the CISO and system administrators.

14.5 Privacy

The Disaster Recovery Policy document shall be considered as "confidential" and shall be made available to the concerned persons with proper access control. Subsequent changes and versions of this document shall be controlled.

14.6 Responsibility

The Disaster Recovery Policy shall be implemented by the CISO / designated personnel.

14.7 Policy

a. Plans for disaster recovery / business resumption / business continuity shall be developed by organizational management.

b. Disaster recovery / business resumption plans shall be updated at least annually and following any significant changes to computing or telecommunications environment of FCI.

c. Employees of FCI shall be trained to execute the disaster recovery plan.

d. Annual certification, updating and testing of the disaster recovery / business resumption plan shall be done.

e. A competent auditor shall audit disaster recovery / business resumption plans.

14.8 Enforcement

Any employee found to have violated this policy may be subjected to disciplinary action in line with the HR Policy / Staff Regulation Act of FCI.

Chapter 15

Change Management Policy

Document Category: Cyber Security Policy

Document Classification: Internal

Access list: All employees of FCI

15.1 Mission Statement

The Change Management Policy shall help to communicate the Management's intent that changes to Information and Communication Technology (ICT) supported business processes will be managed and implemented in a way that shall minimize risk and impact to FCI and its operations.

15.2 Introduction

All changes to IT systems shall be required to follow an established Change Management Process. This requires that changes to IT systems be subject to a formal change management process that ensures or provides for a managed and orderly method by which such changes are requested, approved, communicated prior to implementation (if possible), and logged and tested.

15.3 Purpose

The purpose of this policy is to establish management direction and high-level objectives for change management and control. This policy will ensure the implementation of change management and control strategies to mitigate associated risks such as:

i. Information being corrupted and/or destroyed;
ii. Computer performance being disrupted and/or degraded;
iii. Productivity losses being incurred; and
iv. Exposure to reputation risk.

15.4 Scope

15.4.1 Employees

This policy applies to all parties operating within the organization's network environment or utilizing Information Resources. No employee is exempted from this policy.

15.4.2 IT Assets

This policy covers the data networks, local servers and personal computers (stand-alone or network-enabled), located at FCI offices and depots, where these systems are under the jurisdiction and/or ownership of the organization, and any personal computers, laptops, mobile devices, and servers authorized to access the organization's data networks.

15.4.3 Documentation

The Policy documentation shall consist of Change Management Policy and related procedures and guidelines.

15.4.4 Document Control

The Change Management Policy document and all other referenced documents shall be controlled. Version control shall be used to preserve the latest release and the previous version of any document. However, the previous version of the documents shall be retained only for a period of two years for legal and knowledge preservation purpose.

15.4.5 Records

Records being generated as part of the Change Management Policy shall be retained for a period of two years. Records shall be in hard copy or electronic media. The records shall be owned by the respective system administrators and shall be audited once a year.

15.4.6 Distribution and Maintenance

The Change Management Policy document shall be made available to all the employees covered in the scope. All the changes and new releases of this document shall be made available to the persons concerned. The maintenance responsibility of the document shall be with the CISO and system administrators.

15.5 Privacy

The Change Management Policy document shall be considered as “confidential” and shall be made available to the concerned persons with proper access control. Subsequent changes and versions of this document shall be controlled.

15.6 Responsibility

The CISO / designated personnel is responsible for proper implementation of the Policy.

15.7 Policy

Changes to information resources shall be managed and executed according to a formal change control process. The control process will ensure that changes proposed are reviewed, authorized,

tested, implemented, and released in a controlled manner; and that the status of each proposed change is monitored. In order to fulfill this policy, the following statements shall be adhered to:

a. A current baseline configuration of the information system and its components shall be developed, documented and maintained.

b. A current inventory of the components of the information system along with the ownership shall be developed, documented and maintained.

c. The baseline configuration of the information system shall be updated as an integral part of the information system component installation.

d. Changes to the information system shall be authorized, documented and controlled by the use of formal change control procedure.

e. Changes in configuration of the information system shall be monitored through configuration verification and audit processes.

f. The information system shall be configured to provide only essential capabilities and shall prohibit and /or restrict the use of specific functions, ports, protocols, and/or services. A list of prohibited and/or restricted functions, port, protocols etc. shall be defined and listed.

g. The inventory of the information system components shall be updated as an integral part of the component installation.

h. Automatic mechanism / tools shall be employed to maintain an up-to-date, complete, reliable, accurate and readily available configuration of the information system.

i. Automatic mechanism / tools shall be employed to initiate changes / change request, to notify the appropriate approval authority and to record the approval and implementation details.

j. The information system shall be reviewed at defined frequency to identify and eliminate unnecessary functions, ports, protocols, and/or services.

15.8 Enforcement

Any employee found to have violated this policy may be subjected to disciplinary action in line with the HR Policy / Staff Regulation Act of FCI.

Chapter 16

System Monitoring Policy

Document Category: Cyber Security Policy

Document Classification: Internal

Access list: All employees of FCI

16.1 Mission Statement

To ensure that organizational IT systems are not open to abuse, FCI reserves the right to monitor individual staff usage but only where authorized by senior HR staff and where, in the circumstances, it is fair and appropriate to do so.

16.2 Introduction

A range of monitoring activities need to be established to ensure that the IT systems of FCI are operating efficiently and effectively. This includes the monitoring of information entering, leaving or stored on organizational IT systems. Such monitoring is not, in general, person specific, but employee's personal data may be accessed as part of this policy.

16.3 Purpose

This policy offers guidance regarding monitoring of system use and related user activities. It is intended to guide and inform personnel and help them understand the importance of maintaining logs of all user activities on the system.

16.4 Scope

16.4.1 IT Assets

This policy applies to all organizational information systems and FCI Employees, Contractors, and Third Party Employees, who have access to IT assets of FCI and may be bound by contractual agreements.

16.4.2 Documentation

The System Monitoring Policy documentation shall consist of System Monitoring Policy, related procedures & guidelines.

16.4.3 Document Control

The System Monitoring Policy document and all other referenced documents shall be controlled. The version control shall be used to preserve the latest release and the previous version of any document. However, the previous version of the documents shall be retained only for a period of two years for legal and knowledge preservation purpose.

16.4.4 Records

Records being generated as part of the System Monitoring Policy shall be retained for a period of two years. Records shall be in hard copy or electronic media. The records shall be owned by the respective system administrators and shall be audited once a year.

16.4.5 Distribution and Maintenance

The System Monitoring Policy document shall be made available to all the employees covered in the scope. All the changes and new releases of this document shall be made available to the persons concerned. The maintenance responsibility of the System Monitoring Policy document will be with the CISO and system administrators.

16.5 Privacy

The System Monitoring Policy document shall be considered as "confidential" and shall be made available to the concerned persons with proper access control. Subsequent changes and versions of this document shall be controlled.

16.6 Responsibility

The CISO / designated personnel is responsible for proper implementation of the System Monitoring Policy.

16.7 Policy

Systems shall be monitored to ensure all information security events are recorded. The organization shall comply with all relevant legal requirements applicable to the monitoring and logging activities. System monitoring shall be used as a means to check the effectiveness of controls adopted and also to verify the conformance to the organizational access control and acceptable use policies.

System monitoring shall consider the following aspects:

a. compliance with regulatory and statutory obligations of FCI;
b. effective maintenance of IT systems;
c. prevention or detection of unauthorized use of, or other threats to, organizational IT systems, or criminal activities;
d. compliance with organizational policies and procedures; and

e. review of usage and staff training.

16.8 Enforcement

Any employee found to have violated this policy may be subjected to disciplinary action in line with the HR Policy / Staff Regulation Act of FCI.

Chapter 17

Website Security Policy

Document Category: Cyber Security Policy

Document Classification: Internal

Access list: All employees of FCI

17.1 Mission Statement

To meet the enterprise business objectives and ensure continuity of its operations, FCI shall adopt and follow well-defined and time-tested plans and procedures, to ensure integrity, availability, and authenticity of its website and all information contained within.

17.2 Introduction

An organization's website is its interface with the external world. Information contained within the website is deemed as authentic statements from the management of the organization. It is imperative to publish only authenticated content on the website and maintain its integrity and availability.

17.3 Purpose

The purpose of the Website Security Policy is to establish rules for preserving the integrity, availability, and authenticity of FCI's website.

17.4 Scope

17.4.1 Employees

This applies to all permanent employees, contractual employees, trainees, privileged customers and all other visitors of FCI.

17.4.2 Documentation

The Website Security Policy documentation shall consist of Website Security Policy and related procedures & guidelines.

17.4.3 Document Control

The Website Security Policy document and all other referenced documents shall be controlled. Version control shall be to preserve the latest release and the previous version of any document. However, the previous version of the documents shall be retained only for a period of two years for legal and knowledge preservation purpose.

17.4.4 Records

Records being generated as part of the Website Security Policy shall be retained for a period of two years. Records shall be in hard copy or electronic media. The records shall be owned by the respective system administrators and shall be audited once a year.

17.4.5 Distribution and Maintenance

The Website Security Policy document shall be made available to all the employees covered in the scope. All the changes and new releases of this document shall be made available to the persons concerned. The maintenance responsibility of the Website Security Policy document shall be with the CISO and website administrator.

17.5 Privacy

The Website Security Policy document shall be considered as "confidential" and shall be made available to the concerned persons with proper access control. Subsequent changes and versions of this document shall be controlled.

17.6 Responsibility

The CISO / designated personnel and website administrator are responsible for proper implementation of the Website Security Policy.

17.7 Policy

Following are the policies defined for maintaining Security of FCI's website:

a. The website shall be developed and maintained as per relevant guidelines of Govt. of India.

b. User registration for secured access to FCI's website shall be required when i) a web application or internal link requires user identification before processing, or ii) accessed data has been classified as "sensitive" and requires further authorization.

c. To facilitate site management, information shall be collected for statistical purposes. FCI shall employ software programs to compile summary usage statistics, which may be used for assessing what information is relevant to users. The data so accumulated may be used to help

determine technical design specifications, identify system performance, or pinpoint problem areas.

d. Except for authorized security investigations and data collection, no attempts shall be made to identify individual users or their usage habits. Accumulated data logs will be scheduled for regular deletion in accordance with schedules set by FCI web administrators.

e. Unauthorized attempts to upload information or change website information are strictly prohibited, and may be punishable under relevant cyber laws.

f. Access to sensitive or proprietary business information on FCI websites shall be limited to employees, customers, clients and vendors who have been determined to have an appropriate business reason for having access to such data. All registered website users, who are granted security access, will be identified by a user name (referred to as the User ID). All actions performed with a User ID will be the responsibility of the ID's registered owner.

g. Individuals who are granted password access to restricted information on FCI website are prohibited from sharing those passwords with, or divulging those passwords to, any third parties. User will notify FCI immediately in the event a User ID or password is lost or stolen or if user believes that a non-authorized individual has discovered the User ID or password.

h. FCI's records shall be final and conclusive in all questions concerning whether or not a specific User ID or password was used in connection with a particular action.

i. Any data or document upload to social networking sites shall be duly authorized by the competent authority and shall be done by designated persons authorized to do so.

17.8 Enforcement

Any employee found to have violated this policy may be subjected to disciplinary action in line with the HR Policy / Staff Regulation Act of FCI.

Chapter 18

Technical Vulnerability Management Policy

Document Category: Cyber Security Policy

Document Classification: Internal

Access list: All employees of FCI

18.1 Mission Statement

To meet the enterprise business objectives and ensure continuity of its operations, FCI shall adopt and follow well-defined and time-tested plans and procedures, to ensure that all technical vulnerabilities that exist in the IT systems of FCI are identified and managed.

18.2 Introduction

IT systems contain inherent weaknesses that are termed as vulnerabilities. Threats exploit vulnerabilities to cause harm to IT systems. Hence, it is imperative to regularly identify and plug those vulnerabilities and prevent occurrence of security incidents.

18.3 Purpose

The purpose of the Technical Vulnerability Management Policy is to establish rules and principles for identifying and managing vulnerabilities in IT systems of FCI.

18.4 Scope

18.4.1 IT Assets

This policy applies to all hardware, software, and network assets of FCI.

18.4.2 Documentation

The documentation shall consist of Technical Vulnerability Management Policy and related procedures & guidelines.

18.4.3 Document Control

The Technical Vulnerability Management Policy document and all other referenced documents shall be controlled. Version control shall be to preserve the latest release and the previous version of any document. However, the previous version of the documents shall be retained only for a period of two years for legal and knowledge preservation purpose.

18.4.4 Records

Records being generated as part of the Technical Vulnerability Management Policy shall be retained for a period of two years. Records shall be in hard copy or electronic media. The records shall be owned by the respective system administrators and shall be audited once a year.

18.4.5 Distribution and Maintenance

The Technical Vulnerability Management Policy document shall be made available to all the employees covered in the scope. All the changes and new releases of this document shall be made available to the persons concerned. The maintenance responsibility of the document shall be with the CISO and website administrator.

18.5 Privacy

The Technical Vulnerability Management Policy document shall be considered as "confidential" and shall be made available to the concerned persons with proper access control. Subsequent changes and versions of this document shall be controlled.

18.6 Responsibility

The CISO / designated personnel and system administrator are responsible for proper implementation of the Technical Vulnerability Management Policy.

18.7 Policy

It is the stated goal of FCI to provide secure IT systems and services in order to protect organizational information assets, as well as the privacy of employees, contractors, and third party employees. The timely and consistent application of vendor-supplied security patches or mitigation of a reported vulnerability are critical components in protecting FCI network, systems, and data from damage or loss due to threats such as worms, viruses, data loss, or other types of external or internal attacks.

FCI shall conduct routine scans of its website, servers (including those hosted at NIC), and devices connected to its networks to identify operating system and application vulnerabilities on those devices. FCI requires its system administrators to routinely review the results of vulnerability scans and evaluate, test and mitigate operating system and application vulnerabilities appropriately. Should an administrator identify a reported vulnerability as a potential false positive, the CISO should be notified immediately.

18.8 Enforcement

Any employee found to have violated this policy may be subjected to disciplinary action in line with the HR Policy / Staff Regulation Act of FCI.

Chapter 19

Risk Management Policy

Document Category: Cyber Security Policy

Document Classification: Internal

Access list: All employees of FCI

19.1 Mission Statement

To meet the enterprise business objectives and ensure continuity of its operations, FCI shall adopt and follow well-defined and time-tested plans and procedures, to ensure timely management of organizational risks.

19.2 Introduction

Employees are expected to cooperate fully with any Risk Assessment being conducted on systems for which they are held accountable. Employees are further expected to work with the Risk Assessment Team in the development of a remediation plan.

The policy, and respective procedures, guidelines & forms shall be available to the CISO and members of senior management of FCI.

19.3 Purpose

The purpose of this policy is to identify areas of risk on a timely manner and manage them to ensure continuity of business processes.

19.4 Scope

19.4.1 IT Assets

This policy applies to the entire IT Infrastructure of FCI.

19.4.2 Documentation

The Policy documentation shall consist of Risk Management Policy, Risk Assessment and Treatment Procedure, and related guidelines.

19.4.3 Document Control

The Risk Management Policy document and all other referenced documents shall be controlled. The version control shall be to preserve the latest release and the previous version of any document. However, the previous version of the documents shall be retained only for a period of two years for legal and knowledge preservation purpose.

19.4.4 Records

Records being generated as part of the Risk Management Policy shall be retained for a period of two years. Records shall be in hard copy or electronic media. The records shall be owned by the respective system administrators and shall be audited once a year.

19.4.5 Distribution and Maintenance

The Risk Management Policy document shall be made available to all the employees covered in the scope. All the changes and new releases of this document shall be made available to the persons concerned. The maintenance responsibility of the Risk Management Policy document will be with the CISO and system administrators.

19.5 Privacy

The Risk Management Policy document shall be considered as "confidential" and shall be made available to the concerned persons with proper access control. Subsequent changes and versions of this document shall be controlled.

19.6 Responsibility

The CISO / designated personnel is responsible for proper implementation of the policy.

19.7 Policy

Risk Management Plan shall be drawn by the management which shall identify the people within FCI who will perform risk assessment operations. For this purpose, the events (or series of events) which cause disruption to business processes shall be identified. The risk assessment shall consider probability and impact of such disruptions in terms of time, scale of damage and recovery period. The risk assessment shall identify, quantify and prioritize risks against criteria and objectives relevant to the organization, including critical resources, impacts of disruptions, allowable outage times and recovery priorities. Based on the results of the assessment, business continuity strategy shall be outlined for FCI to determine overall approach to business continuity.

19.8 Enforcement

Any employee found to have violated this policy may be subjected to disciplinary action in line with the HR Policy / Staff Regulation Act of FCI.

Chapter 20

Incident Management Policy

Document Category: Cyber Security Policy

Document Classification: Internal

Access list: All employees of FCI

20.1 Mission Statement

Incident Management policy shall enable response to a major incident or disaster by implementing a plan to restore the critical business functions of FCI.

20.2 Introduction

The number of computer security incidents and the resulting cost of business disruption and service restoration rise with increase in dependence on IT-enabled processes. Implementation of sound security policies, blocking of unnecessary access to networks and computers, improvement in user security awareness, and early detection and mitigation of security incidents are some of the actions that can be taken to reduce such risks and decrease the cost of security incidents.

20.3 Purpose

The purpose of the incident management policy is to provide organization-wide guidance to employees on proper response to, and efficient and timely reporting of, computer security related incidents, such as computer viruses, unauthorized user activity, and suspected compromise of data. It also addresses non-IT incidents such as power failure. Further, this policy provides guidance regarding the need for developing and maintaining an incident management process within FCI.

20.4 Scope

20.4.1 Employees

This policy applies to all FCI Employees, Contractors, and Third Party Employees, who use, process, and manage information from individual systems or servers.

20.4.2 Documentation

The documentation shall consist of Incident Management Policy, and related procedures & guidelines.

20.4.3 Document Control

The Incident Management Policy document and all other referenced documents shall be controlled. Version control shall be to preserve the latest release and the previous version of any document.

However, the previous version of the documents shall be retained only for a period of two years for legal and knowledge preservation purpose.

20.4.4 Records

Records being generated as part of the Incident Management Policy shall be retained for a period of two years. Records shall be in hard copy or electronic media. The records shall be owned by the respective system administrators and shall be audited once a year.

20.4.5 Distribution and Maintenance

The Incident Management Policy document shall be made available to all the employees covered in the scope. All the changes and new releases of this document shall be made available to the persons concerned. The maintenance responsibility of the document shall be with the CISO and system administrators.

20.5 Privacy

The Incident Management Policy document shall be considered as "confidential" and shall be made available to the concerned persons with proper access control. Subsequent changes and versions of this document shall be controlled.

20.6 Responsibility

The Incident Management Policy shall be implemented by the CISO / designated personnel.

20.7 Policy

The organizational management shall ensure that:

a. Incidents are detected as soon as possible and properly reported.

b. Incidents are handled by appropriate authorized personnel with 'skilled' backup as required.

c. Incidents are properly recorded and documented.

d. All evidence is gathered, recorded and maintained in the Security Incident Reporting form that will withstand internal and external scrutiny.

e. The full extent and implications relating to an incident are understood.

f. Incidents are dealt with in a timely manner and service(s) restored as soon as possible.

g. Similar incidents will not recur.

h. Any weaknesses in procedures or policies are identified and addressed.

i. The risk to FCI's reputation through negative exposure is minimized.

j. All incidents shall be analyzed and reported to the designated officer(s).

k. Learning from the incidents are recorded.

The policy shall apply throughout the organization, including information resources, data stored and processed on those systems, data communication and transmission media, and personnel who use information resources.

20.8 Enforcement

Any employee found to have violated this policy may be subjected to disciplinary action in line with the HR Policy / Staff Regulation Act of FCI.

Chapter 21

Physical Security Policy

Document Category: Cyber Security Policy

Document Classification: Internal

Access list: All employees of FCI

21.1 Mission Statement

To meet the enterprise business objectives and ensure continuity of its operations, FCI shall adopt and follow well-defined and time-tested plans and procedures, to ensure physical security of all information assets and human assets.

21.2 Introduction

Physical security is an essential part of a security plan. It forms the basis for all other security efforts, including personnel and information security. A balanced security programme must include a solid physical security foundation. A solid physical security foundation protects and preserves information, physical assets and human assets.

21.3 Purpose

The purpose of the Physical Security Policy is to:

a. establish the rules for granting, control, monitoring, and removal of physical access to FCI office premises;
b. to identify sensitive areas within the organization; and
c. to define and restrict access to the same.

21.4 Scope

21.4.1 Employees

This applies to all permanent employees, contractual employees, trainees, privileged customers and all other visitors of FCI.

21.4.2 Documentation

The Physical Security Policy documentation shall consist of Physical Security Policy and related procedures & guidelines.

21.4.3 Document Control

The Physical Security Policy document and all other referenced documents shall be controlled. Version control shall be to preserve the latest release and the previous version of any document.

However, the previous version of the documents shall be retained only for a period of two years for legal and knowledge preservation purpose.

21.4.4 Records

Records being generated as part of the Physical Security Policy shall be retained for a period of two years. Records shall be in hard copy or electronic media. The records shall be owned by the respective system administrators and shall be audited once a year.

21.4.5 Distribution and Maintenance

The Physical Security Policy document shall be made available to all the employees covered in the scope. All the changes and new releases of this document shall be made available to the persons concerned. The maintenance responsibility of the Physical Security Policy document will be with the CISO and system administrators.

21.5 Privacy

The Physical Security Policy document shall be considered as "confidential" and shall be made available to the concerned persons with proper access control. Subsequent changes and versions of this document shall be controlled.

21.6 Responsibility

The CISO / designated personnel is responsible for proper implementation of the Physical Security Policy.

21.7 Policy

Following are the policies defined for maintaining Physical Security in FCI:

a. Physical access to the server rooms / areas shall completely be controlled and servers shall be kept in the server racks under lock and key.

b. Access to the servers shall be restricted only to designated Systems and Operations Personnel. Besides them, if any other person wants to work on the servers from the development area then he / she shall be able to connect to the servers only through Remote Desktop Connection with a Restricted User Account.

c. Critical backup media shall be kept in a fire proof off-site location in a vault.

d. Security perimeters shall be developed to protect areas that contain information system to prevent unauthorized physical access, damage and interference.

e. A list of personnel with authorized access to the facilities where information systems reside shall be maintained with appropriate authorization credentials. The access list and authorization credentials shall be reviewed and approved by authorized personnel periodically.

f. All physical access points (including designated entry / exit points) to the facilities where information systems reside shall be controlled and access shall be granted to individuals after verification of access authorization.

g. Physical access to the information systems shall be monitored to detect and respond to physical security incidents.

h. Physical protection against damage from fire, flood, earthquake, explosion, civil unrest and other forms of natural and man-made disasters shall be designed and applied.

i. Physical protection and guidelines for working in the areas where information systems resides shall be designed and applied.

j. Information systems and their components shall be positioned within the facility to minimize risks from physical and environmental hazards and opportunity for unauthorized access.

k. Information systems shall be protected from power failure and other disruptions caused by failure in supporting utilities.

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

m. The real-time physical intrusion alarm and surveillance equipment shall be monitored.

n. Physical access control to information systems shall be independent of the physical access control to the facility. This control can be applicable to server rooms or information systems with higher impact level than that of the majority of the facility.

o. Automated mechanisms to recognize potential intrusion shall be employed to initiate appropriate response actions.

p. Physical access to the information systems shall be granted only after authenticating visitors before authorizing access to the facility where the information systems reside other than areas designated as "publicly accessible".

q. The access records of the visitors shall be maintained.

r. Visitors shall be escorted by the designated personnel and their activities, if required, shall be monitored.

s. Systems Personnel shall examine laptops of visitors for latest anti-virus definition, latest patches and updates, and any sort of vulnerability which could be harmful for the FCI network.

t. Any user who needs to connect to external network for official work shall be able to do so after an official sanction from FCI Management and Security Team. This team shall evaluate security risks before issue of any sanction.

u. A record of all physical accesses by both visitors and authorized individuals shall be maintained.

v. All policies stated above shall be monitored for any changes from time to time.

21.8 Enforcement

Any employee found to have violated this policy may be subjected to disciplinary action in line with the HR Policy / Staff Regulation Act of FCI.

Chapter 22

Network Services Security Policy

Document Category: Cyber Security Policy

Document Classification: Internal

Access list: All employees of FCI

22.1 Mission Statement

To meet the enterprise business objectives and ensure continuity of its operations, FCI shall adopt and follow well-defined and time-tested plans and procedures, to ensure protection of its network services.

22.2 Introduction

To support its business functions, FCI encourages the use of, and provides access to, information technologies and network resources. This enables employees to access global information resources, as well as the ability to communicate with other users worldwide. In keeping with its role and values, FCI supports the use of electronic communication for the conduct of official business and for individual professional needs.

22.3 Purpose

The purpose of this policy is to protect the integrity and availability of networked services.

22.4 Scope

22.4.1 IT Assets

This policy applies to all organizational network systems, end devices which access networks and information systems of FCI.

22.4.2 Documentation

The documentation shall consist of Network Services Security Policy, and related procedures & guidelines.

22.4.3 Document Control

The Network Services Security Policy document and all other referenced documents shall be controlled. Version control shall be to preserve the latest release and the previous version of any document. However, the previous version of the documents shall be retained only for a period of two years for legal and knowledge preservation purpose.

22.4.4 Records

Records being generated as part of the Network Services Security Policy shall be retained for a period of two years. Records shall be in hard copy or electronic media. The records shall be owned by the respective system administrators and shall be audited once a year.

22.4.5 Distribution and Maintenance

The Network Services Security Policy document shall be made available to all the employees covered in the scope. All the changes and new releases of this document shall be made available to the persons concerned. The maintenance responsibility of the document shall be with the CISO and system administrators.

22.5 Privacy

The Network Services Security Policy document shall be considered as "confidential" and shall be made available to the concerned persons with proper access control. Subsequent changes and versions of this document shall be controlled.

22.6 Responsibility

The Network Services Security Policy shall be implemented by the CISO / designated personnel and network administrator.

22.7 Policy

The organizational network shall be designed and configured to deliver high performance and reliability to meet the needs of the business whilst providing a high degree of access control and a range of privilege restrictions. Suitably qualified staff shall be designated to manage the organization's network, and preserve its integrity in collaboration with the nominated individual system owners. The networks and networked services, which are allowed to be accessed, shall be clearly specified. There shall be an authorization process for determining who shall be allowed to access which networks and networked services. Unauthorized access to network connections and network services shall be minimized.

22.8 Enforcement

Any employee found to have violated this policy may be subjected to disciplinary action in line with the HR Policy / Staff Regulation Act of FCI.

Chapter 23

Outsourcing and Supplier Policy

Document Category: Cyber Security Policy

Document Classification: Internal

Access list: All employees of FCI

23.1 Mission Statement

All contracts with external suppliers for providing services to FCI shall be monitored and reviewed to ensure that information security requirements are being satisfied. Contracts shall include appropriate provisions to ensure the continued security of information and systems in the event that a contract is terminated or transferred to another party.

23.2 Introduction

Outsourcing and Supplier Policy sets out the conditions that are required to maintain the security of the information and systems of FCI when third parties other than the organization's own staff are involved in their operation. This may occur in at least three distinct circumstances:

a. When third parties (for example, contractors) are involved in the design, development or operation of information systems for the organization. There may be many reasons for this to happen, including developing and installing bespoke software, third party maintenance or operation of systems, to full outsourcing of an IT facility;

b. When access to the organization's information systems is granted from remote locations where computer and network facilities may not be under the control of the organization;

c. When users who are not members of the organization are given access to information or information systems.

Each of these circumstances involves a risk to the organization's information, which should be assessed before the third party is granted access. Such access must be subject to appropriate conditions and controls to ensure that risks can be managed.

23.3 Purpose

The Outsourcing and Supplier Policy sets out the conditions that are required to maintain the security of the organization's information and systems when third parties are involved in their operation.

23.4 Scope

23.4.1 Employees

This policy applies to all Suppliers, Contractors, and Third Parties who provide IT-related services to FCI.

23.4.2 IT Assets

This policy is applicable for all network systems, services and information systems of FCI.

23.4.3 Documentation

The documentation shall consist of Outsourcing and Supplier Policy, and related procedures & guidelines.

23.4.4 Document Control

The Outsourcing and Supplier Policy document and all other referenced documents shall be controlled. Version control shall be to preserve the latest release and the previous version of any document. However, the previous version of the documents shall be retained only for a period of two years for legal and knowledge preservation purpose.

23.4.5 Records

Records being generated as part of the Outsourcing and Supplier Policy shall be retained for a period of two years. Records shall be in hard copy or electronic media. The records shall be owned by the respective system administrators and shall be audited once a year.

23.4.6 Distribution and Maintenance

The Outsourcing and Supplier Policy document shall be made available to all the employees covered in the scope. All the changes and new releases of this document shall be made available to the persons concerned. The maintenance responsibility of the document shall be with the CISO and system administrators.

23.5 Privacy

The Outsourcing and Supplier Policy document shall be considered as "confidential" and shall be made available to the concerned persons with proper access control. Subsequent changes and versions of this document shall be controlled.

23.6 Responsibility

The Outsourcing and Supplier Policy shall be implemented by the CISO / designated personnel.

23.7 Policy

a. All third parties who are given access to FCI's information systems, whether suppliers, customers or others, must agree to follow the organization's information security policies. A summary of the information security policies of FCI and the third party's role in ensuring compliance will be provided to any such third party, prior to their being granted access.

b. FCI shall assess the risk to its information assets and, where deemed appropriate because of the confidentiality, sensitivity or value of the information being disclosed or made accessible, FCI shall require external suppliers of services to sign a confidentiality agreement to protect its information assets.

c. Persons responsible for agreeing to maintenance and support contracts shall ensure that the contracts being signed are in accordance with the content and spirit of FCI's information security policies.

d. All contracts with external suppliers for the supply of services to FCI must be monitored and reviewed to ensure that information security requirements are being satisfied. Contracts must include appropriate provisions to ensure the continued security of information and systems in the event that a contract is terminated or transferred to another supplier.

e. Any facilities management, outsourcing or similar organization, with which FCI may do business, must be able to demonstrate compliance with FCI's information security policies and enter into binding Service Level Agreements (SLAs) that specify the performance to be delivered and the remedies available in case of non-compliance.

23.8 Enforcement

Any employee found to have violated this policy may be subjected to disciplinary action in line with the HR Policy / Staff Regulation Act of FCI.

Chapter 24

Compliance Policy

Document Category: Cyber Security Policy

Document Classification: Internal

Access list: All employees of FCI

24.1 Mission Statement

FCI is committed to managing its legal and contractual compliance obligations in a proactive, ongoing and responsible manner. It is committed to not only identifying the legislation which it is obliged to comply with but also measuring the levels of compliance in the organization.

24.2 Introduction

A Legal and Contractual Compliance Programme is a system for identifying and monitoring compliance with legislation and contractual agreements. It also attempts to raise employee awareness of legal and contractual obligations and aims to embed a compliance culture within the organization.

24.3 Purpose

This policy provides guidance to prevent breaches of any criminal and civil law, statutory, regulatory or contractual obligations.

24.4 Scope

24.4.1 Employees

This policy applies to all FCI Employees, Contractors, and Third Party Employees, who use, process, and manage information and business processes of FCI.

24.4.2 Documentation

The documentation shall consist of Compliance Policy, and related procedures & guidelines.

24.4.3 Document Control

The Compliance Policy document and all other referenced documents shall be controlled. Version control shall be to preserve the latest release and the previous version of any document. However, the previous version of the documents shall be retained only for a period of two years for legal and knowledge preservation purpose.

24.4.4 Records

Records being generated as part of the Compliance Policy shall be retained for a period of two years. Records shall be in hard copy or electronic media. The records shall be owned by the respective system administrators and shall be audited once a year.

24.4.5 Distribution and Maintenance

The Compliance Policy document shall be made available to all the employees covered in the scope. All the changes and new releases of this document shall be made available to the persons concerned. The maintenance responsibility of the document shall be with the CISO and system administrators.

24.5 Privacy

The Compliance Policy document shall be considered as "confidential" and shall be made available to the concerned persons with proper access control. Subsequent changes and versions of this document shall be controlled.

24.6 Responsibility

The Compliance Policy shall be implemented by the CISO / designated personnel and Compliance Officer (if any).

24.7 Policy

The organization shall explicitly define and document its approach to meet all legal, regulatory and contractual requirements. Issues of data protection, restrictions on use of specific technology, compliance with security policies and standards must be defined and documented. Legal advice shall be sought and all above mentioned documents shall be kept up to date.

24.8 Enforcement

Any employee found to have violated this policy may be subjected to disciplinary action in line with the HR Policy / Staff Regulation Act of FCI.