Version History

Ver. No.	*Authors*	*Date*	*Reviewers*	*Review Date*	*Release Date*
1.0	CISO	27-Aug-2018	ISMF	31-Aug-2018	03-Sep-2018
1.1	CISO	11-Feb-2019	ISMF	11-Feb-2019	11-Feb-2019
2.0	CISO	11-Dec-2019	ISMF	13-Dec-2019	16 -Dec-2019
2.1	CISO	11-Aug-2020	ISMF	13-Aug-2020	14-Aug-2020
3.0	CISO	02-Nov-2020	ISMF	06-Nov-2020	10-Nov-2020

Change History

Ver. No.	*Section*	*Date*	*Change Information*	*RFC No.*
1.0	All	03-Sep-2018	New Release	-
1.1	PO – 07	11-Feb-2019	Addition of CCTV details in Physical & Environmental Policy	Document Modification Form
2.0	All	16-Dec-2019	Annual Release	-
2.1	13.2.1	11-Aug-2020	Background verification clause and scope updated in the ISMS manual - HR Policy – 13.2.1	Client Suggestion
3.0	All	10-Nov-2020	Annual Review	-

Table of Content

Introduction

0.1 Background:

- CIPL is planning its Business Processes automation using integrated technology solutions and to become extensively IT enabled organization. This integrated technology setup needs to be regulated to meet some of the accepted best practices of IT governance using Policies and Procedures
- A well detailed policies and procedures are essential to ensure a reasonable degree of information system integrity and risk mitigation framework from a best practices stand point.
- **The following policies are to be adopted by CIPL:**

Policies	Policy #
Information Security	PO-01
Information Security Management Framework	PO-02
Employee Access Control	PO-03
Security Organization	PO-04
Asset Management	PO-05
Access Control	PO-06
Physical & Environmental	PO-07
Password Management	PO-08
Incident Management	PO-09
Disposal of Media	PO-10
Internal Audit	PO-11
Compliance	PO-12
Human Resource Security	PO-13
Acceptable Use of Assets	PO-14
Communication	PO-15
Email	PO-16
Network Management	PO-17
Internet	PO-18
Anti-Virus	PO-19
Mobile Computing Devices Security	PO-20
Backup	PO-21
Patch Management	PO-22
Change Management	PO-23
Desktop	PO-24
Daily Monitoring	PO-25
BCP DR	PO-26
Procurement of HW/SW/Services	PO-27
Network Time Synchronization	PO-28
Vulnerability Management	PO-29
Management Review	PO-30

Policies	Policy #
Corrective Action	PO-31
Capacity Management	PO-32
Clear Desk Clear Screen	PO-33
Monitoring and Measurement	PO-34
Cryptography	PO-35

1. Information Security Policy – PO–01

1.1 Purpose

The purpose of this information security policy is to prescribe mechanism that will assist in identifying, preventing, detecting, and correcting the compromise and misuse of the CIPL's information and Information Technology infrastructure.

1.2 Policy Details

1.2.1 Security Policy

CIPL's information systems and the business information therein are assets of strategic and commercial value. They are fundamentals to the efficient business continuity.

CIPL shall implement controls to ensure:

- Information assets and IT assets are protected against unauthorized access.
- Information is not disclosed to unauthorized persons through deliberate or careless action.
- Information is protected from unauthorized modification.
- Information is available to authorized users when needed.
- Applicable regulatory and legislative requirements are met.
- Disaster recovery plans for IT assets are developed, maintained and tested as far as practicable.
- Information security training is imparted to all IT users.
- All breaches of information security are reported and investigated.
- Violations of policies are dealt with a disciplinary action.

1.2.2 Security Policy

To protect assets from all threats, whether internal or external, deliberate or accidental, CIPL will take measures to ensure that:

- *Information will be **protected against unauthorized access***
- ***Confidentiality** of Information is assured*
- ***Integrity** of Information is maintained*
- ***Availability of information and information systems will be met***
- ***Regulatory** and **legislative** requirements will be met*
- ***Business Continuity plans** will be produced, maintained and tested*
- *Necessary **training** will be offered to maintain information security*
- ***Incident management** process will be practiced to **keep damage to minimum** and to **prevent the recurrence** of the same*
- ***Internal policies and procedures** will be **reviewed periodically** for **continuous improvement***
- ***Establish User Guidelines stating Do's and Don'ts** related to usage of internet,*

email, computer system and measures taken for data protection

- ***Senior management to L1 level employee,*** *all are* ***equally responsible*** *for* ***implementing and adhering information security policies*** *within their scope of deliverables.*

Mr. Javed Tapia

Managing Director

1.2.3 CIPL provides following services to its clients:

1.2.3.1 System Processes:

- Management Review
- Internal Audit
- Corrective Action
- Document Control
- Monitoring and Measurement
- Customer Complaint
- Risk Assessment
- Change Management

1.2.3.2 Operations Processes

- Human Resources
- Administration
- Information Technology
- Application Development
- Operations

Following are the locations included under the scope of the ISMS:

- Mumbai

To support these activities the huge Information and communication infrastructure is established in CIPL organization, which has importance to its business. To ensure efficient functioning, uninterrupted availability and security of the above infrastructure and information, it is imperative that the guidelines for the procurement, upkeep, maintenance, utilization and security of the above are laid down clearly and monitored closely. This Policy provides requirements for the safety and security of its information assets.

Security is everyone's business and 'Security Consciousness' is the foundation for harmonious running of an organization. Security discipline must be continuously practiced and experienced during peacetime so that it becomes way of life and automatic during wartime. The security of an establishment depends upon the vigilance of all its personnel in general and the security staff in particular. It is the duty of all personnel to ensure that while they themselves do nothing towards

the prejudice of information, personnel and material, they also do everything in their power to safeguard the same.

1.3 Communication of Policy Details

This policy and relevant specific policies, procedures shall be published on Company's Intranet and communicated to employees and relevant external parties by emails.

1.4 Periodical Review

The information security policy shall be reviewed on yearly basis or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

The Information Security Management Forum would review this Policy, the compliance and implementation status, effectiveness of controls and their implementation, taking into account Internal Audit Reports, Incidents, suggestions and feedback from related parties and make appropriate recommendation for improvements.

1.5 Violation of the Information Security Policy

Non-compliance or violation of the CIPL's Information Security policy shall result in disciplinary action as per the CIPL's Human Resource Policy and other such rules prevalent at the time of violation.

1.6 ISO controls

- A.5.1.1 Policies for Information security
- A.5.1.2 Review of the Policies for information security

1.7 References

- Human Resource Policy

2. Information Security Management System Framework Policy – PO–02

2.1 Purpose

The purpose of this Information Security Management System Framework is to prescribe mechanism that will assist in establishing, maintaining, updating the Policies / Processes in CIPL to ensure smooth working of all operations.

2.2 Policy Details

2.2.1 Information Security Requirements

2.2.1.1 Business Requirements

Information Technology is integral part of CIPL's business processes. Information in any form is thus most valuable asset for CIPL. The list and type of assets are mentioned in scope of ISMS. CIPL has its own policies and procedures to deal with security standard to handle the important documents.

2.2.1.2 Contractual obligations:

- Provide services worldwide on 24 * 5 * 365 basis
- The NON disclosure agreements service deliver agreements or service providers including details about IPR, copyrights of the material shared by customers/service providers to CIPL and delivered to customers/service providers by CIPL.

2.2.1.3 Legal and regulatory requirements

CIPL has identified and maintained list of laws to comply with such as:

- The Arbitration and Conciliation Act, 1996
- The Banker's Books Evidence Act, 1891
- The Banking Regulation Act, 1949
- The Civil Procedure Code, 1908
- The Code of Criminal Procedure, 1973
- The Companies Act 1956
- The Consumer Protection Act, 1986
- The Copyright Act 1957
- The Essential Commodities Act, 1955
- The Foreign Exchange Management Act, 1999
- The Hindu Succession Act, 1956
- The Income Tax Act 1961
- Indian Contract Act 1872
- Indian Evidence Act
- Indian Partnership Act, 1932
- Indian Penal Code 1862
- The Indian Trusts Act, 1882
- The Indian Stamp Act, 1899

- The Indian Succession Act
- The Industrial Disputes Act, 1947
- The Information Technology Act 2008
- The Limitation Act, 1963
- The Negotiable Instruments Act, 1881
- The Notaries Act, 1952
- The Patents Act, 1970
- The Power of Attorney Act, 1882
- The Prevention of Money Laundering Act 2002
- The Registration Act, 1908
- The Reserve [organization type] of India Act
- The Trade Marks Act, 1999
- The Employee's Compensation (Amendment) Act, 2017
- Sexual Harassment of Women at Workplace (Prevention, Prohibition, and Redressal) Act, 2013
- The Payment Of Wages (Amendment) Act, 2017
- The Payment of Bonus (Amendment) Ordinance, 2007
- Maharashtra Shops and Establishments (Regulation of Employment and Conditions of Service) Act, 2017

Recognizing the need of security of information assets according to security requirements above and related systems for its processing, transmission and storage, CIPL has initialized various measures.

Settings up and operating information security Management (ISMS) is one of such initiatives. This documents explains the approach of CIPL in formalizing ISMS under following heads

- Establishing and managing ISMS
- Implementing and operating ISMS
- Monitoring and Reviewing ISMS
- Maintaining and improving ISMS

2.2.1.4 Establishing and Managing ISMS

- **Scope of ISMS**

"CIPL is directed to establish an Information Security Management Program, consistent with prudent business practice with the goal of adequately providing quality & secured services to the customers with efforts to exceed the expectations."

- **Information Security Management System at CIPL is applicable to the following:**

System Processes:

- Management Review
- Internal Audit
- Corrective Action
- Document Control
- Monitoring and Measurement

- Customer Complaint
- Risk Assessment
- Change Management

Operations Processes

- Human Resources
- Administration
- Information Technology
- Application Development
- Operations

Following are the locations included under the scope of the ISMS:

- Mumbai

- **Risk Assessments Methodology**

The objectives of assessing the risk are to identify the risk to which IT assets and information assets are exposed. Risk is the function of value of the asset at risk, the severity of the threat and likelihood of threats, exploiting vulnerability.

CIPL aims to reduce the risk factors of all its information assets to an acceptable level, such that company's people and business are not affected. "Acceptable Risk" is the risk level that the management of CIPL is prepared to accept as business risk. For details regarding the Risk assessment methodology, derivation of their acceptable risk level and the criteria for risk acceptance, please refer Risk Assessment Policy and Risk Assessment Procedure.

Following key elements were considered while performing risk assessment:

- The unique set of security risk, which could lead to significant losses to business, if they occur. This depends upon the risk associated with the information assets and the level of criticality of these information assets to the company's business.
- The statutory and contractual requirements to be satisfied by CIPL, which includes legal compliances, intellectual property Rights, safeguarding of companies records and data protection.
- The security requirements relating to the organization-wide principals, objectives and requirements for information processing to support its business operations.

- **Risk assessment process**

For Risk assessments process, please refer "Risk Assessments Procedure". Broadly CIPL has taken following steps:

- Identifying, listing ascertaining ownership and classification of key information assets and information processing assets.
- Valuation assets
- Identification of security requirements

- Assessments of threats and vulnerabilities
- Assessments of statutory and contractual requirements
- Assessments of organization wide principles, objectives and business requirements
- Measurement of risk
- Risk management
- Risk treatments plan

- **Identification of information assets and information process assets**

Information in any form is an asset. An asset is something's that has value or utility to the organization, its business operations and its continuity. The proper management and accountability of information assets is vital in order to maintain appropriate protection. As a corollary, all assets that aid in information processing are also to be appropriately protected to ensure security of the information assets.

Please refer "Assets Register" documents for an exhaustive list of all assets.

- **Ownership of information assets**

The person or departments that creates the documents or information, is the owner of that particular information.

- Ownership of CIPL's main IT network infrastructure and software assets is with CISO
- Ownership of communication facilities such as telephones lines with Administration / IT Department
- Ownership of physical access control systems, services(utilities such as power supply, water supply etc., Access cards) to the IT infrastructure is with Administration department
- Owner of each information asset is mentioned against each asset as documented in above mentioned document.

- **Classification of information assets**

CIPL would be a role model for having robust Information Security Management System Implementation with continual improvements, which assure and pervade every sphere of its activities and functional domains.

- **Valuation of key information assets**

Empowerment of Information Security Management System shall be through implementation of best practices for People, Process and Technology.

- **Risk Ratings**

The purpose of this Information Security Policy is to prescribe mechanism that will assist in identifying, preventing, detecting, and correcting the compromise and misuse of the CIPL's information and Information Technology infrastructure.

- **Risk management**

The scope will be as per ISMS scope defined in ISMS-01 Scope of ISMS document.

- **Selection of controls objectives:**

  - Information Security is the responsibility of everyone in the CIPL.
  - The Information Security Information Security Management Forum shall have the responsibility to establish, review and implement Information Security Management System (ISMS).
  - Chief Information Security Officer (CISO) shall be responsible for successful implementation of ISMS in the organization.
  - Information Security Management Forum shall review and update the Security Policies, Processes and Procedures.
  - Information Security Task force shall implement and maintain the controls.
  - All Department heads will be directly responsible for ensuring compliance of the policies in their departments.

2.2.2 Security Statement

CIPL's information systems and the business information therein are assets of strategic and commercial value. They are fundamentals to the efficient business continuity.

CIPL shall implement controls to ensure:

- Information assets and IT assets are protected against unauthorized access.
- Information is not disclosed to unauthorized persons through deliberate or careless action.
- Information is protected from unauthorized modification.
- Information is available to authorized users when needed.
- Applicable regulatory and legislative requirements are met.
- Disaster recovery plans for IT assets are developed, maintained and tested as far as practicable.
- Information security training is imparted to all IT users.
- All breaches of information security are reported and investigated.
- Violations of policies are dealt with a disciplinary action.

2.3 Communication of Policy Details

This policy and relevant specific policies, procedures shall be published on Company's Intranet and communicated to employees and relevant external parties by emails.

2.4 Periodical Review

The information security policy shall be reviewed on yearly basis or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

The Information Security Management Forum would review this Policy, the compliance and implementation status, effectiveness of controls and their implementation, taking into account Internal Audit Reports, Incidents, suggestions and feedback from related parties and make appropriate recommendation for improvements.

2.5 Violation of the Information Security Policy

Non-compliance or violation of the CIPL's Information Security policy shall result in disciplinary action as per the CIPL's Human Resource Policy and other such rules prevalent at the time of violation.

2.6 ISO controls

- Not Applicable

2.7 References

- Risk Assessment Policy
- Human Resource Policy
- Risk Assessment Procedure Human Resource Policy

3. Employee Access Policy – PO – 03

3.1 Purpose

The objective of the policy is to manage logical user access to "Information" within CIPL by ensuring that the access is provided on a "Need to Know", "Need to Do" basis and is in line with the business requirements defined by the various departments.

3.2 Policy Details:

These policies are applicable for all the information enablers i.e. business applications, support applications, operating systems, file and print servers, and Databases etc.

3.2.1 User id Creation:

All users shall be created on the basis of business requirement stated in the User Registration Form and duly approved by the respective departmental head and resource owner.

3.2.2 User Registration will be centrally handled by the IT team:

- All users shall be provided with unique user IDs (both at application and system level) and shall follow a standard naming convention.
- The group Ids shall be used in case access has to be provided to a group or role for specific business requirements

3.2.3 User Id Deletion Policy:

- IT shall be informed by the HR Department of the employee's discharge so that access rights of such employees can be withdrawn.
- An employee shall be relieved only on getting a clearance from the concerned departments, which has allocated resources to the user.
- HR shall approve the handover form which shall initiate action for disabling the access rights of the concerned employee
- The process for deleting user access rights will be the following:
    - Process of closing / deleting an account shall be initiated by the HR department in following cases:
        - Termination of an employee
        - Resignation of an employee
        - Retirement of an employee
    - On all these cases, HR shall inform IT as well as the concerned Head of the Department the departure date of the employee
    - IT Team shall ensure that the necessary business data is backed up before initiating de-allocation
- IT shall get the details and accordingly the access profiles shall be removed and all resources assigned to the employee shall get de allocated
- IT shall change the passwords of all online services used by CIPL and intimate to all other concerned users

- For temporary staff, consultants and other third party having system access, the concerned department head shall be responsible for ensuring that the HR initiates the access deletion process in the way mentioned above.

3.2.4 Temporary Disabling of User Accounts:

- Users may go on vacation during which period the account may be accessed by unauthorized entities. Users shall be educated to inform the system administrator to disable their account for the period of absence.
- User accounts of users who go on leave for more than 10 days shall be disabled.
- System shall disable accounts idle for more than 10 days
- For disabled accounts the user activation shall comply with the User Id Creation Policy

3.2.5 Account Lock out Policy:

- Wherever possible, the user id shall be disabled if the password is entered 10 times unsuccessfully

3.2.6 Access Privilege Change Policy – Permanent:

- Any change in the access privileges of any user shall be done through a formal process
- The process for changing the access privileges of a user shall be the same as the User Id Creation Policy

3.2.7 Access Privilege Change Policy – Temporary:

- Whenever a user goes on extended leave, it may be required to give another user, of a different privilege, the same privileges as the user who went on leave. This may be required to ensure that responsibilities carried out by the user who is on leave continues to be carried out
- Temporary change in access privilege shall be carried out only if there is a shortage of staff caused by an employee taking long leave. The duration of such changes shall be restricted to appropriate periods of time
- There shall be a formal authorization process for the temporary change in work class to be carried out
- A log of all temporary changes made shall be maintained and periodically reviewed

3.3 Communication of Policy Details

This policy and relevant specific policies, procedures shall be published on Company's Intranet and communicated to employees and relevant external parties by emails.

3.4 Periodical Review

The information security policy shall be reviewed on yearly basis or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

The Information Security Management Forum would review this Policy, the compliance and implementation status, effectiveness of controls and their implementation, taking into account Internal Audit Reports, Incidents, suggestions and feedback from related parties and make appropriate recommendation for improvements.

3.5 Violation of the Information Security Policy

Non-compliance or violation of the CIPL's Information Security policy shall result in disciplinary action as per the CIPL's Human Resource Policy and other such rules prevalent at the time of violation.

3.6 ISO controls

- A.5.2.2 – Training, awareness and competence
- A.12.3.1 – Information Backup
- A.12.4.1 – Audit Logging
- A.12.4.2 – protection of log information
- A.12.4.3 – administration and operator logs
- A.12.4.1 – Monitoring system uses
- A.9.2. – User access Management Control of Technical Vulnerability

3.7 References

- Human Resource Policy
- Information Security Policy
- Information Asset Classification and Handling Policy
- Risk Assessments Procedure

4. Security Organization Policy – PO – 04

4.1 Purpose

This policy lays down the formal security organization structure with clearly defined roles, responsibilities and accountabilities

4.2 Policy Details

4.2.1 Scope

This policy shall be applicable to all those employees of CIPL who are part of Information Security organization.

4.2.2 Policy Statement

- An Information Security Management Forum constituted by the CIPL shall give a clear direction and management support for information security initiatives within CIPL.
- The Chief Information Security Officer (CISO) shall be responsible for information security within CIPL. (Ref. A.6.1.3)
- ISMS (Information Security Management System) Forum shall be formed which shall be responsible for coordinating the implementation of information security within organization and its management. This forum will comprise of representatives from different business functions and locations.
- Information Security Task Force shall be responsible for coordination of ISMS related activities throughout the organization.
- The Information Security Management Forum shall release/ change Information Security policy.
- The CISO, based on the organization's needs and the type of incidents, shall seek specialist security advice from internal or external consultants.
- The CISO shall implement ISMS in the organization with the help of various position/s having their individual/collective role and responsibility in the ISMS framework as defined in Security Organization Structure.

4.3 Communication of Policy Details

This policy and relevant specific policies, procedures shall be published on Company's Intranet and communicated to employees and relevant external parties.

4.4 Periodical Review

The information security policy shall be reviewed on yearly basis or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

The Information Security Management Forum would review this Policy, the compliance and implementation status, effectiveness of controls and their implementation, taking into account Internal Audit Reports, Incidents, suggestions and feedback from related parties and make appropriate recommendation for improvements.

4.5 Violation of the Information Security Policy

Non-compliance or violation of the CIPL's Information Security policy shall result in disciplinary action as per the CIPL's Human Resource Policy and other such rules prevalent at the time of violation.

4.6 ISO controls

- A.6.1.3 – Allocation of information security responsibilities

4.7 References

- Information Security Policy
- Human Resource Policy

5. Asset Management Policy – PO – 05

5.1 Purpose

All IT assets used by CIPL are owned by CIPL. A large amount of company's internal, confidential & critical information is created and stored or supported by these IT assets and systems. CIPL will ensure all feasible efforts to maintain appropriate access control and availability of these assets. This policy is developed for classification of the IT Assets and systems so that appropriate controls can be implemented based on the threat to the asset.

The purpose of this document is to provide guidance to CIPL businesses on (a) classifying information generated or used by the Company; and (b) recommended ways to label, store, transmit, and dispose of such information, depending on its classification.

5.2 Policy Details

5.2.1 Scope

All IT assets and systems which includes but not limited to Desktops, Laptops, Servers and network components, software assets (including applications), power supply, UPS, HVAC (Heat, Ventilation, Air conditioning units), Fire detection and suppression systems, EPABX shall fall within one of the following three classifications based on their ability to affect the company's ability to deliver services and the ability to protect the confidentiality of information assets.

This policy applies to employees, contract employees and consultants at CIPL, including all personnel affiliated with any third parties. This policy applies to all information that is owned or leased by CIPL

5.2.2 Policy Statement

Each IT asset of CIPL handled by its users and / or administrators, and support staff will be classified and labeled either as highly critical or moderately critical or non-critical asset. Access control to these systems will adhere to the guidelines set in the access control policy.

5.2.3 Asset Classification

- **Highly Critical:**

  Information of the highest sensitivity, if mishandled may cause substantial damage to the CIPL's business / image. For e.g. merger/acquisition information, strategic business plans, customer transaction information, etc.

- **Moderately Critical:**

  Information, which, if mishandled, may cause moderate damage to the CIPL's business / image e.g. departmental budget plans, customer information, personnel information, internal memos, telephone books, organization charts etc.

- **Non-Critical:**

  Information, which, even if mishandled, may not cause damage to the CIPL's business / goodwill e.g., annual report, already published product information brochures, etc.

5.2.4 Asset Labeling and Handling

- The assets shall be classified and clearly labelled so that all users are aware of the ownership and classification of the asset.
- From the time when IT asset is acquired until it is destroyed or declassified, it must be labelled (marked) with a sensitivity designation.
- Information and its related IT assets shall be processed and stored strictly in accordance with the classification levels assigned to those assets.
- Access to the information assets shall be the responsibility of a designated owner or custodian.

5.2.5 Information Asset Classification

All information on the CIPL Information Systems shall be classified based on its importance to its business and to its image. The classification of information may change over a period and necessary controls shall be applied.

5.2.6 Definition

Information: Any information, which has value, usefulness and association to CIPL.

Information Owner: Any person or persons, individually or collectively responsible at Group Head levels for any subset of the data or the information on the Organizations Information Systems.

Information Custodian: Any person or persons, individually or collectively responsible to perform regular administrative tasks on the information delegated by the information owner or Information Security Task Force.

5.2.7 Information ownership and accountability

Manager IT shall designate a person or group of persons to be responsible for an asset. Such person or group of persons shall be the Asset owner. Ownership of the asset remains with the owner at any level however, different persons, processes shall be held accountable for compromising the confidentiality, integrity and / or availability of information, hence detective controls shall be in place wherever possible.

5.2.8 Classification of information

Information classification shall be classified based on confidentially, integrity and availability by their respective owners into any one of the following:

(a) Confidential
(b) Restricted
(c) Company Circulation

The above classifications are defined as follows:

(a) Confidential

This classification applies to the sensitive organizational or departmental information that is

intended strictly for use within limited group of individuals within the department. Its unauthorized disclosure and / or access could seriously and adversely impact the organization and will have to be treated with care. This type of information shall be handled using controlled access to address confidentiality.

(b) Restricted

This classification applies to sensitive business information that is intended strictly for use within the Group. This information shall be exempted from any disclosure and / or access rules or other applicable laws or regulations. Its unauthorized disclosure and / or access could seriously and adversely impact the Group and its stakeholders, its business partners, and / or its customers and will have to be treated with care. Access shall be granted only to group members or authorized individuals.

(c) Company Circulation

This classification applies to information that is intended for use within the Department. Its unauthorized disclosure could moderately impact the Organization and / or its employees.

5.2.9 Roles and Responsibilities of Information Owners

The Information owner shall:

(a) Maintain an appropriate level of protection, physical and / or logical, for the information.
(b) Take prior approval of the IT Manager or Group Head before sharing information.
(c) Review the information classification periodically.
(d) Ensure availability of information at all times and circumstances.
(e) Periodic review of access control.

The Information custodian shall:

(a) Perform regular backup and data validity testing activities.
(b) Perform data restoration from backups periodically.
(c) Implement access control as defined by information owner.
(d) Perform regular administrative tasks.

Document#: Label	Company circulation	Restricted	Confidential
General Description	Information belonging to the Department and not for disclosure to the public or external parties. Generally available to employees and authorized non-employees of the department	Information that is sensitive or private, of highest value to the group, and intended for use within the group only.	Information that is sensitive or confidential and of highest value to the Company and intended for business use and only for those with a need-to know.

Document#: Label	Company circulation	Restricted	Confidential
Examples	Company organization charts and telephone directories	Individually identifiable customer or client information / data; cost or pricing information;	Merger/acquisition-related information; major trade secrets; strategic plans; financial results prior to release; trade-controlled information; files containing clear-text passwords,
Impact of Unauthorized Disclosure	Limited harm	Significant harm (e.g., financial liability, adverse competitive impact, harm to Company reputation)	Severe harm (e.g., financial liability, extreme harm to competitive position; significant harm to Company reputation
Physical Labeling (Paper, CD/DVD or Tape Label)	Company Circulation	Restricted	Confidential
Electronic Labeling (Digital File, E-mail, or Web Page)	"Company Circulation" on subject-line or header / footer required.	"Restricted" on subject-line or header / footer required.	"Confidential" on subject-line or header / footer required
Physical Storage (Paper or Tape)	Secure cabinets or other drawers. Room need not be locked if access to the department is restricted for Its department employees and authorized non-employees only.	Storage in a locked drawer, file cabinet, or office recommended, but not required.	Secure office. Storage in a locked drawer, file cabinet, or office required. If stored in an open-file storage area, access to the area must be restricted to authorized personnel.
Electronic	Stored in a directory	Properly locked up and access controlled	Properly locked up and access controlled

5.3 Communication of Policy Details

This policy and relevant specific policies, procedures shall be published on Company's Intranet and communicated to employees and relevant external parties.

5.4 Periodical Review

The information security policy shall be reviewed on yearly basis or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

The Information Security Management Forum would review this Policy, the compliance and implementation status, effectiveness of controls and their implementation, taking into account Internal Audit Reports, Incidents, suggestions and feedback from related parties and make appropriate recommendation for improvements.

5.5 Violation of the Information Security Policy

Non-compliance or violation of the CIPL's Information Security policy shall result in disciplinary action as per the CIPL's Human Resource Policy and other such rules prevalent at the time of violation.

5.6 ISO controls

- A.8.2.1 Classification guidelines
- A.8.2.2 Information labelling

5.7 References

- Human Resource Policy

6. Access Control Policy – PO – 06

6.1 Purpose

This policy addresses role based logical access control to various Information resources and services in CIPL to ensure that strict and appropriate controls are in place and access to all information resources and services is controlled as per business requirements Policy Details.

6.2 Policy Details

This policy applies to employees and non-employees associated with CIPL who access or administer access to information resources. This policy covers all the Information systems, applications and IT resources owned by CIPL.

6.2.1 Policy Statement

Each IT asset of CIPL handled by its users and / or administrators, and support staff will be classified and labeled either as highly critical or moderately critical or non-critical asset. Access control to these systems will adhere to the guidelines set in the access control policy.

6.2.2 Access Control Policy – Logical

6.2.2.1 Access to information shall be controlled based on (Ref. A.9.1.1):

- Business requirements
- Need to know basis
- Need to perform tasks basis
- Information Asset Classification and Handling Policy

6.2.2.2 The access control policy –

Access control policy logical shall be in accordance with the ISMS policy and shall be reviewed once every six months and / or if any major changes in application or business requirement. (Ref. A.9.1.1)

6.2.2.3 The Management

The user management will be done in accordance with CIPL's exiting Access Control Policy, which shall be defined for management of user access to Information assets such as (Ref. A.9.2):

- Application Software
- Computing Devices e.g. Server, Desktop, Laptop etc.
- Services e.g. Internet, Intranet, E-mail
- Network
- Storage Devices
- Printers
- Scanners

6.2.2.4 All Users

All the users to whom the access to Information system shall be provided, a using Service Now Tool for User ID Creation with detailed information has to be provided in the approved Email by the Department Head. Department Head has to send the Email to concerned Information Technology department who will create the ID's. Based on this the User shall be provided the access to information assets of CIPL. (Ref. A.9.2.1)

6.2.2.5 The user-ID created shall be (Ref. A.9.5.2)

- Unique in nature
- Have an authentication mechanism
- Have defined and approved requirement
- Have appropriate and approved access / privileges to information Resource

6.2.2.6 The user-ID privileges shall be managed as requested by Department Head and in accordance to ISMS security policy. Any addition or removal of all or partial privileges shall be taken care of by PR-03 Access Control Procedure. (Ref. A.9.2.3)

6.2.2.7 Every user shall be given an Initial password while creating the user-ID and will be informed to change the password immediately before using the information system assets through that user-ID. This is to protect the password secrecy. (Ref. A.9.2.4)

6.2.2.8 User-ID access rights shall be reviewed every time when the user has internal transfer, as specified in PR-13 Human Resource Procedure. (Ref. A.9.2.5)

6.2.2.9 Generic User-IDs shall exist for administrators of specific applications / systems only.

6.2.2.10 User shall be made aware of their responsibilities while working in organization Network (Ref.11.3) such as:

- Password secrecy (Ref.A.9.3.1)
- Clear desk clear screen (Ref.A.11.2.9)
- Unattended equipment's (Ref.A.11.2.8)

6.2.2.11 Violation of access control policy shall call for punitive action as per the organizations Human Resource Policy. (Ref. A.9.2.3)

6.2.2.12 OS level and Network level controls shall be established to protect un-authorized logical access to IT Infrastructure. (Ref. A.9.4.2)

6.2.2.13 The users shall be provided access to different system using their user IDs. The control shall be established wherever possible so that intruder / imposter shall not be able to override system and application controls. (Ref. A.9.4.4)

6.2.2.14 All users shall follow Password policy to protect his interest along with CIPL.

6.2.2.15 Network Operating System logon to domain through desktops shall be in a secured manner so as to:

- Unattended user equipment such as desktops shall be locked and revoked with password (Ref. A.11.2.8)

6.2.2.16 Other equipment shall be controlled with appropriate protection (Ref. A.11.3.2)

6.2.2.17 Access to production files and databases shall be made through Service Now Tool approved by IT Manager and Department Head (Ref. A.11.2.9)

6.2.2.18 Concerned Department Head or Information Technology Department, after approval from IT Manager, shall revoke the privileges of a user under the following circumstances (Ref. A.9.2.3):

- Any conduct that is deemed as interfering with the normal and proper operation of the organization's information systems
- Any conduct that is deemed to adversely affect the ability of others to use the information systems
- Any conduct that is deemed to be harmful or offensive to others
- Termination of service/transfer of user

6.2.2.19 All User ID's that have not been used for a specific period, shall be temporarily suspended, disabled, and / or reset. (Ref. A.9.4.2)

6.2.2.20 Wherever possible all secure login and logout controls provided with the operating system shall be configured to protect the security of Information system. (Ref. A.9.4.2)

- Display a general notice warning that authorized users shall only access the system (Ref. A.9.4.2)
- Limit the number of three in application systems and five in windows logins unsuccessful attempts and then shall be automatically locked.

6.3 Communication of Policy Details

This policy and relevant specific policies, procedures shall be published on Company's Intranet and communicated to employees and relevant external parties.

6.4 Periodical Review

The information security policy shall be reviewed on yearly basis or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

The Information Security Management Forum would review this Policy, the compliance and implementation status, effectiveness of controls and their implementation, taking into account Internal Audit Reports, Incidents, suggestions and feedback from related parties and make appropriate recommendation for improvements.

6.5 Violation of the Information Security Policy

Non-compliance or violation of the CIPL's Information Security policy shall result in disciplinary action as per the CIPL's Human Resource Policy and other such rules prevalent at the time of violation.

6.6 ISO Control

- A.9.1.1 Access Control Policy.
- A.9.2.1 /A9.2.2 User Registration.

- A.9.2.3 Privilege Management.
- A.9.2.4 User Password Management.
- A.9.2.5 Review of User Access Right.
- A.9.3.1 Password Use.
- A.11.2.8 Unattended User Equipment.
- A.11.2.9 Clear Desk and Clear Screen Policy.
- A.9.4.2 Secure Log-on Procedure.
- A.9.2.1 User Identification and Authentication.
- A.9.4.4 Use of System Utilities.
- A.9.4.2 Session Time-out.
- A.9.4.2 Limitation of Connection Time.
- A.9.4.1 Information Access Restriction.

6.7 References

- Information Security Policy
- Asset Classification and Handling Policy
- Password Policy
- Access Control Procedure - Logical
- Password Procedure
- Human Resource Procedure
- Change Management Procedure

7. Physical & Environmental – PO – 07

7.1 Purpose

This policy addresses all the aspects involved in prevention of unauthorized physical access, theft, damage and interference to information and IT systems / assets, which lead to interruption of business activities.

7.2 Policy Details

This policy applies to employees and non-employees associated with the CIPL who access or administer access to information resources.

7.2.1 Policy Statement

This policy shall cover all the IT systems, applications and IT resources owned by CIPL and installed at data center.

7.2.2 Access Control Policy – Physical

- Physical Security in CIPL building is controlled by Admin Department in accordance with Security requirements defined by Management.
- Physical Security for Data Centre in CIPL is controlled by Technology Department with Admin Department.
- A list of all sensitive areas shall be maintained by Admin / Technology Department for administration purpose. Sensitive areas shall be defined and marked as follows:
  - Restricted Area: This shall be the area where 'Critical' / 'Highly critical' / 'Confidential' information / assets are stored / processed.
  - Employee Work Area: This shall be the area where employees work and information classified as 'Restricted', is stored / processed.
- Visibility of the restricted areas from outside the premises shall be avoided. (Ref. A.11.1.3)
- Strict access control shall be established in restricted areas. (Ref. A.11.1.2)
- 'Restricted Area' shall be protected from natural and man-made incidences such as Fire, Flood, civil unrest, and man-made disaster. (Ref. A.11.1.4)
- Appropriate working instructions (Do's and Don'ts) shall be displayed on entry for 'Restricted Area'. (Ref. A.11.1.5)
- Delivery and loading areas pertaining to IT equipment shall be separated from information processing facilities (Ref. A.11.1.6)
- Identification badges / Access Card shall be issued to all employees and non-employees (contractors and third party personnel) for access to CIPL premises. All employees and non-employees shall visibly display the badges while in any CIPL premises.
- Access to 'Restricted area' shall be controlled as described in Restricted Area Access Procedure in PR-07 Access Control Procedure - Physical.
- The information assets, equipment's / IT assets which are classified as "Highly Critical" shall be protected from environmental threats and hazards and un-authorized access. (Ref. A.9.2.1).
- Any incidents related to physical security breach resulting in un-authorized access shall be reported to Security Help Desk for incident management.
- All the IT equipment's that are identified, as "Highly Critical" and the same shall be provided with redundant backup in case of failure of equipment's or supporting utilities. (Ref. A.11.2.2)
- Alternative manual access control system in case of power failure for electronic access control system, shall be established (Ref. A.11.2.2)
- The power, telecommunication and data cabling shall be protected wherever possible from interceptions and damages. The necessary distance between power and data cables wherever possible shall be maintained to protect data loss in transit. (Ref. A.11.2.3)

- The equipments shall be maintained periodically to ensure its continuous availability and integrity. (Ref. A.11.2.4)
- All users shall store all the media and documents in lock and key to protect from un-authorized access.
- All the equipments and media shall be taken off-site with proper authorization and record to this effect shall be maintained by Admin Department. (Ref. A.11.2.5, A.8.3.1)
- Access to Lock and Key cabinet shall be given only after proper authorization and proper Key management procedure shall be defined for unauthorized access to Lock and Key cabinet.
- The security protection such as Tamperproof packaging / Sealed Envelope shall be provided when the equipments or media is taken out from CIPL premises through personally/ reliable courier/transport agency for repairs or for working outside. (Ref. A.11.2.6, A.8.3.3)
- Any media or device shall be checked to ensure that any critical/ highly critical data and / or licensed software on it are securely overwritten prior to disposal. (Ref. A.11.2.7)
- Incoming / Outgoing IT material shall be checked. (Ref. A.11.2.5)
- CCTV shall be installed to monitor activities at the respecting working areas
- CCTV footage shall be backed up and shall be maintained for 30 days
- Information storing and processing equipment shall be protected from (Ref. A.11.2):
  - Loss
  - Damage
  - Compromise
  - Interception
  - Power failure

7.3 Communication of Policy Details

This policy and relevant specific policies, procedures shall be published on Company's Intranet and communicated to employees and relevant external parties.

7.4 Periodical Review

The information security policy shall be reviewed on yearly basis or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

The Information Security Management Forum would review this Policy, the compliance and implementation status, effectiveness of controls and their implementation, taking into account Internal Audit Reports, Incidents, suggestions and feedback from related parties and make appropriate recommendation for improvements.

7.5 Violation of the Information Security Policy

Non-compliance or violation of the CIPL's Information Security policy shall result in disciplinary action as per the CIPL's Human Resource Policy and other such rules prevalent at the time of violation.

7.6 ISO Control

- A.11.1.2 – Physical entry controls
- A.11.1.3- securing office, room and facilities

- A.11.1.4 – protecting against external end environmental threats
- A.11.1.5- working in secure area
- A.11.1.6- delivery and loading areas
- A.11.2.1- equipment sitting and protection
- A.11.2.2- supporting utilities
- A.11.2.3-cabling security
- A.11.2.4-Equipment maintenance
- A.11.2.6-security of equipment and assets off premises
- A.11.2.7- security disposal or re-use of equipment
- A.11.2.5- removal of assets
- A.8.3.1- Management of Removable Media
- A.8.3.3 – Physical media transfer
- A.11.2.9- clear desk and clear screen policy

7.7 References

- Access Control Procedure
- Human Resource Procedure

8. Password Management Policy– PO – 08

8.1 Purpose

The objective of this policy is to ensure that access to the information assets is restricted to authorized users only. The users are identified through unique user IDs to establish accountability and non-repudiation. Good password procedures are enforced through the systems. The users are made aware about their responsibilities for selection and usage of their user IDs and passwords.

8.2 Policy Details

The policy applies to:

- All CIPL employees / users' information assets including external support agencies, that operate, manage, use or access, in any form, the Information Technology (IT) assets of the CIPL.
- All systems, applications, databases, Network components and other IT assets.

8.2.1 Policy Statement

To protect access to CIPL's Information Assets, users of Information Systems shall be provided with unique user identification and access shall be authenticated through the use of passwords to ensure security and non-repudiation.

8.2.2 Use of Non-unique / Generic User IDs and Password

- Password entries shall be masked to prevent visibility to any User Critical Use
- A generic User Identification and Password may be utilized for access to critical shared or common area workstations like 'root' so long as
    - The usage as well as the users are documented and authorized by the Head of the Information Technology Department.
    - A record of password change shall be maintained.
- The passwords shall be kept in sealed cover envelopes. A Record of revealing password shall be maintained.

8.2.3 Initial Default Password

- Hard coding of passwords, within applications, shall be prohibited.
- Auto / Blank password Logins shall be disabled for all user IDs.
- All initial / default passwords shall be changed before migrating the system into the production environment.
- All initial passwords shall be changed at the time of first login. Wherever possible, this shall be enforced through the system, otherwise, it shall be followed by the users procedurally.
- In case of certain critical assets, where the default passwords for certain login-IDs cannot be changed or the default passwords are deemed necessary, then in such cases, specific exceptions shall be authorized by Manager IT.

8.2.4 Password Complexity

- All passwords used to gain access to the information assets shall be of sufficient complexity to ensure that they are not easily guessable and must have the following characteristics.
    - Length: Passwords must be a minimum of eight characters in length.
    - Type: Passwords must incorporate the following characters:
        - At least one lower case character (a-z)
        - At least one upper case character (A-Z)
        - At least one number (0-9)
    - In addition to the above, passwords for access to critical assets shall include at least one special character found on a standard ASCII keyboard e.g.! @ # $ % ^ & * ( ) _ - + = { } [ ] : ; “ ‘ | \ / ? < > , . ~ ` etc.
    - It should not consist of consecutive identical characters.
    - It should not be any date format, month of year, day of week
    - It should not be same as user name or user Id or personal information.
    - Passwords should not be dictionary words (English or Marathi / local language equivalents).

8.2.5 Password Change Management

- Change in Team Composition
- Passwords shall be changed immediately on the change in composition of the team owning / sharing that password e.g. root password shall be immediately changed if there is a change in the team of system administrators.
- Knowledge of Disclosure
    - Password must be changed if it is suspected that it has been disclosed or compromised.
- Time
    - Password aging times may be implemented in a manner commensurate with the criticality and sensitivity of the information asset but shall not exceed three months.
    - Where change of passwords cannot be systemically enforced, the users shall procedurally change it at defined periods.
- User capability to change passwords
    - Users shall be provided with the capability to change their password.
    - Passwords must not be disclosed to other users or individuals.
    - Users must not allow other users or individuals to use their password, including when on vacation.
- Passwords must not be written down, posted, or exposed in an insecure manner such as on a notepad or posted on the workstation.
- Passwords should be stored in secured manner. (Ref. A. 9.5.3)

8.2.6 Account Lockout and Reactivation

- Lockout

- Locking of Passwords for unsuccessful login attempts will be applicable to respective business applications.
- In case of critical logins, exceptions must be documented and approved by Manager IT

- Re-activation
  - In case of a login account being locked out, the Project Manager working as System Administrator shall reactivate the same on receipt of properly authorized written request.

8.2.7 Reset of Password

Properly authorized Password Reset Requests shall be submitted to the security administrator using ticketing software.

8.2.8 User Responsibility

- Users shall not use the "Password Remember" feature of applications.
- Access to information assets shall be through authorized user IDs allocated as per the Access Control Policy.
- Users shall be responsible for the proper use and protection of their passwords and access to the Information Assets through their User Ids. (Ref. A.9.3.1)
- Passwords shall be used only for legitimate access to networks, systems, or applications and shall be treated as Critical and Confidential Information. (Ref.A.9.2.4) (Ref. A.9.4.3)

8.3 Communication of Policy Details

This policy and relevant specific policies, procedures shall be published on Company's Intranet and communicated to employees and relevant external parties.

8.4 Periodical Review

The information security policy shall be reviewed on yearly basis or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

The Information Security Management Forum would review this Policy, the compliance and implementation status, effectiveness of controls and their implementation, taking into account Internal Audit Reports, Incidents, suggestions and feedback from related parties and make appropriate recommendation for improvements.

8.5 Violation of the Information Security Policy

Non-compliance or violation of the CIPL's Information Security policy shall result in disciplinary action as per the CIPL's Human Resource Policy and other such rules prevalent at the time of violation.

8.6 ISO controls

- A.9.2.4 Use password management

- A.9.3.1 Password use
- A.9.4.3 Password management system.

8.7 References

- Information Security Policy
- Human Resource Policy

9. Incident Management Policy – PO – 09

9.1 Purpose

This policy addresses the issue of detecting, logging, escalating / reporting and resolving Information security Incidents and weaknesses in timely manner with the intent to minimize the damage arising out of violation of security policies and misuse of information systems and related assets and support services.

9.2 Policy Details

The scope of this policy covers all Information Security Incidents as defined below, and is applicable to all employees, contractors and third party personnel who use information systems, related assets and support services of CIPL.

9.1.1 Definitions

- IT Security Incident: IT security incident is defined as any event, which has a notable negative impact on the Organization's information security. An IT security incident falls under any of the following types:
  - Unauthorized access into Organization's IT Systems (such as intrusion, virus attack, etc.)
  - Exploitation of security weaknesses / vulnerabilities
  - Software and hardware malfunctions
  - Misuse of information systems resources
  - Violation of Organization's policies and procedures
  - Violation of applicable legal laws and other regulatory conditions
  - Human Errors
  - Uncontrolled system changes
  - Service, facility or equipment loss

- Non-IT Security Incident: Non-IT security incident is defined as any event, which has a notable negative impact on the Organization's information security and information/IT assets and is non-technical in nature such as:
  - Lapse in physical security
  - Thefts
  - Fire
  - Environmental hazards

9.1.2 Policy Statement

- A formal Information Security Incident Management Procedure shall be defined and implemented by the ISMS forum to aid this policy. (Ref. A.16.1.2)

- All Information Security Incidents shall be classified to facilitate monitoring, assigning and reporting. Information Security Incident classification shall be done based on the Fault Category and the priority. (Ref.A.16.1.2)
- CIPL shall establish contacts with Special Interest groups in Information Security such as CERT (Worldwide, India), ISACA and law enforcement agency such as Cyber Crime cell, Hyderabad for exchange of information, receive early warnings of alerts, update knowledge base, understand best practices in handling security incidences etc. (Ref.A.6.1.4)
- The organization has the right to monitor the usage of all information assets / services / facilities.
- Users shall report all Information Security Incidents pertaining to information security and weaknesses through the Information Security Incident Management Procedure. (Ref.A.16.1.3)
- Users shall not report to or discuss Information Security Incidents with other un-authorized users or persons external to the organization.
- Any attempt to interfere with, prevent, obstruct or dissuade employees in their efforts to report actual / suspected information, whether on account of accidental or intentional acts or violations committed by self or others to those rightfully investigating is strictly prohibited and would be liable for disciplinary action.
- Technology Department / Departmental (Functional) representative shall have access to all critical servers to monitor system use, ensuring that only authorized actions and processes are performed.
- Technology Department shall maintain accurate computer system clock to ensure the accuracy of audit logs, which may be needed for investigation or as evidence in legal or disciplinary cases. Where a computer or communications device uses a real-time clock, it shall be set to local standard time. Clock timings shall be regularly checked and synchronized with standard local time.
- Different types of intrusion detection products shall be installed to detect and warn of attacks.
- In the event of detecting a suspected attack, actions shall be taken to prevent further attempts
- A formal disciplinary process shall be in place for handling violations of security policies and procedures. These disciplinary processes would be in line with Acceptable Use Policy and related 'Human Resource Policy'.
- All Information Security Incidents shall be resolved to ensure that: (Ref.A.16.1.1)
  - The occurrence of such incidents are minimized or eliminated and
  - Effective security controls are strengthened and re-established
- Learning from Information Security Incidents shall be captured and stored appropriately and shall be disseminated to Technology Department / Security / Users. (Ref.A.16.1.6)
- Wherever possible, evidence shall be collected to initiate and support such disciplinary action and later if required prosecution process for violating legal requirements including the Organization's policies and procedures, and emphasis shall be given to ensure that these evidences are fully admissible in the court of law. (Ref.A.16.1.7)
- Information Security incidents, if required to be communicated to outside authorities / Press, shall be reported by Authorized person in consultation with Manager IT.

9.3 Communication of Policy Details

This policy and relevant specific policies, procedures shall be published on Company's Intranet and communicated to employees and relevant external parties.

9.4 Periodical Review

The information security policy shall be reviewed on yearly basis or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

The Information Security Management Forum would review this Policy, the compliance and implementation status, effectiveness of controls and their implementation, taking into account Internal Audit Reports, Incidents, suggestions and feedback from related parties and make appropriate recommendation for improvements.

9.5 Violation of the Information Security Policy

Non-compliance or violation of the CIPL's Information Security policy shall result in disciplinary action as per the CIPL's Human Resource Policy and other such rules prevalent at the time of violation.

9.6 ISO Control

- A.6.1.4 Contact with special interest groups.
- A.16.1.2 Reporting information security events
- A.16.1.3 Reporting security weaknesses
- A.16.1.1 Responsibilities and procedures
- A.16.1.6 Learning from information security incidents
- A.16.1.7 Collection of evidence

9.7 References

- Information Security Policy
- Human Resource Policy
- Change Management Policy
- Information Security Incident Management Procedure

10. Disposal of Media Policy – PO – 10

10.1 Purpose

The purpose of this policy is to establish a standard for the proper and secured disposal of electronic media and computing devices containing information / data to minimize the risk of information leakage to unauthorized persons.

10.2 Policy Details

This policy covers all media types like but not limited to Hard disk, CD, DVD, Floppy diskettes, USB, PDA, Zip Disks, Tapes and access Cards etc.

10.1.1 Policy Statement

- There shall be a formal Disposal of Electronic Media and Computing Devices Procedure. (Ref. A.8.3.2 & Ref. A.11.2.7)
- The information useful to organization and requires retention shall be backed-up before disposal of Electronic Media and Computing Devices. (Ref.A.8.3.1)
- ISMS Task Force shall be responsible for disposal of electronic media and computer devices.
- All electronic media and computing devices identified for disposal shall be erased, degaussed, or rendered unusable before taken out of the organization.
- Disposal of electronic media shall comply with existing environmental and other applicable regulations.
- The register shall be maintained to record the Disposal of electronic media and computing devices.

10.3 Communication of Policy Details

This policy and relevant specific policies, procedures shall be published on Company's Intranet and communicated to employees and relevant external parties.

10.4 Periodical Review

The information security policy shall be reviewed on yearly basis or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

The Information Security Management Forum would review this Policy, the compliance and implementation status, effectiveness of controls and their implementation, taking into account Internal Audit Reports, Incidents, suggestions and feedback from related parties and make appropriate recommendation for improvements.

10.5 Violation of the Information Security Policy

Non-compliance or violation of the CIPL's Information Security policy shall result in disciplinary action as per the CIPL's Human Resource Policy and other such rules prevalent at the time of violation.

10.6 ISO Controls

- A.11.2.7 Secure disposal or re-use of equipment
- A.8.3.1 Management of removable media
- A.8.3.2 Disposal of media

10.7 References

- Information Security Policy
- Human Resource Policy
- Disposal of Electronic Media and computing Devices Procedure

11. Internal Audit Policy – PO – 11

11.1 Purpose

The purpose of this policy is to establish a standard for internal security audit to be conducted by Audit committee to ensure confidentiality, integrity and availability of information assets and information processing resources complying with the Organizations security policies and to report Audit findings.

11.2 Policy Details

This policy covers the entire IT infrastructure owned and operated by CIPL

11.1.1 Policy Statement

- Audit Committee shall conduct internal security audits in the Organization for compliance with ISO 27001:2013 standard and other relevant statuary compliances defined by the compliance Policy.
- The internal audit committee shall conduct regular internal audit after every six months
- Internal audit committee will oversee the audit conducted by auditors
- To have a proper segregation of duties, the audit and implementation activities will be separated.
- The internal Audit Team members shall consider the compliance report of previous internal audit and external audit report
- During audit monitoring and review of third party services, adherence to agreement, incidents related to third party, reports and records generated during process etc. shall be carried our(A.15.2.1)
- An internal Audit procedure shall be prepared by the audit committee and approved by the ISMS forum
- On request and approval from a competent authority, the audit team may be granted access to
    - User level and / or system level access to any computing or communication device
    - Access to information (electronic, hardcopy etc.) that may be produced or transmitted or stored on organizations equipment or premises

- Access to work areas (Data center, offices, cubicles, desk drawers, storage areas)
- Access to interactively monitor and log traffic on organizations Network

- The audit committee shall submit an audit report to the ISMS Forum after completion of the each audit along with relevant evidences.
- The ISMS Forum shall review audit report submitted by the audit committee and shall take appropriate corrective actions.

11.3 Communication of Policy Details

This policy and relevant specific policies, procedures shall be published on Company's Intranet and communicated to employees and relevant external parties.

11.4 Periodical Review

The information security policy shall be reviewed on yearly basis or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

The Information Security Management Forum would review this Policy, the compliance and implementation status, effectiveness of controls and their implementation, taking into account Internal Audit Reports, Incidents, suggestions and feedback from related parties and make appropriate recommendation for improvements.

11.5 Violation of the Information Security Policy

Non-compliance or violation of the CIPL's Information Security policy shall result in disciplinary action as per the CIPL's Human Resource Policy and other such rules prevalent at the time of violation.

11.6 ISO Controls

- A.15.2.1 Monitoring and review of third party services
- A.15.3. Information system audit considerations
- A.12.7.1 Information system audit controls

11.7 References

- Information Security Policy
- Internal Audit Procedure
- Corrective Action Procedure
- Management Review Procedure

12. Compliance Policy – PO – 12

12.1 Purpose

This policy addresses the compliance requirements pertaining to relevant statutory legislations, contractual and regulatory obligations and CIPL's information security policies with respect to information security.

12.2 Policy Details

This policy shall be applicable to all departments, functions and employees of CIPL.

12.2.1 Policy Statement

- ISMS Forum shall identify statutory, legal and contractual requirements pertaining to information systems. (Ref. A.15.1)
- HR / Admin Department shall communicate (Ref.18.1.2):
  - Compliance with all relevant applicable laws and regulations related to information security for all premises of CIPL.
  - Legal restrictions imposed by Intellectual Property Rights (IPR) and copyright.
- ISMF Forum shall adhere with the Intellectual Property Rights (IPR) act and shall arrange for acquisition of Copyright software. (Ref.18.1.2)
- Protect the Organizations records in any form as classified in Asset Classification based on retention, storage, handling and disposal. (Ref. A.18.1.3)
- Department Head shall take action to ensure that all applicable laws and regulations related to information security are complied with respect to their areas of operations.
- Any use of Information and Information Assets for non-business use shall be prohibited.
- Department Head and ISMS Forum shall ensure adherence of information security policies of CIPL within their area of operations. (Ref.18.1.3)
- Audit Committee shall undertake periodic audits of all premises to ensure compliance with CIPL's security policies.
- ISMS Forum, at least once in a year, shall conduct technical compliance checks like penetration testing, application / System testing and vulnerability assessment of critical information assets.
- ISMS Forum shall enforce ISMS Policy throughout the Organization to avoid security breaches. (Ref.18.2.2)
- ISMS shall have regular review of compliance of ISMS policy and incidences reported shall have a corrective action, followed by review. (Ref. A.18.2.2)
- ISMS Forum in co-ordination with Internal Audit Committee shall make all the necessary arrangement required for Information System Audit, without disturbing to business processes. (Ref.12.7.1)
- Any external person caring out the Information system Audit, using Audit tools, shall be considered as third party, physical access controls and risk involved to business process shall be evaluated.

12.3 Communication of Policy Details

This policy and relevant specific policies, procedures shall be published on Company's Intranet and communicated to employees and relevant external parties.

12.4 Periodical Review

The information security policy shall be reviewed on yearly basis or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

The Information Security Management Forum would review this Policy, the compliance and implementation status, effectiveness of controls and their implementation, taking into account Internal Audit Reports, Incidents, suggestions and feedback from related parties and make appropriate recommendation for improvements.

12.5 Violation of the Information Security Policy

Non-compliance or violation of the CIPL's Information Security policy shall result in disciplinary action as per the CIPL's Human Resource Policy and other such rules prevalent at the time of violation.

12.6 ISO Controls

- A.18.1.2 Intellectual Property Right (IPR)
- A.18.1.3 Protection of organization record
- A.18.2.2 Compliance with security policies and procedures
- A.12.7.1 Information systems audit controls

12.7 References

- Information Security Policy
- Internal Audit Policy
- Human Resource Policy
- Compliance Procedure

13. Human Resource Policy – PO – 13

13.1 Purpose

This policy discusses about implementing ISMS security controls to ensure that employees, contractors and third party users shall understand their roles and responsibilities for which they are considered for, before the employment, during the employment and after termination or change of employment.

13.2 Policy Details

This policy shall be applicable to all Human Resource Department of CIPL.

13.2.1 Policy Statement

- The roles and responsibilities of employees, contractors and third party users shall be defined and documented. (Ref. A.6.1.1)
- Formal procedure shall exist for recruitment based on CIPL's requirement such as appropriate qualifications and experience; pre-recruitment screening and background checks; relevant laws, regulations and ethics. (Ref. A7.1.1)
    - Background Verification - The joinees during the on-boarding process, provides details for his prior 2 employments as per the verification format.
    - The employment verification is initiated with all the previous employment as per the details provided.
    - The HR member takes the last 2 employment details and forwards the same to their Third-party verification vendor
    - The Third-party conducts verification as per the set process. The Third-party vendor submits the verification report for the respective resources individually
    - The status report is checked and if the response is negative, appropriate action is initiated and the details are filed in the employee file
    - If the status report has a positive response, the same is reviewed and filled in the respective employee's personal file.
- All the employees, contractors and third party shall agree and sign the terms and conditions of appointment and Non-Disclosure Agreement, which include their organizational responsibilities for Information Security during and after contract term. (Ref. A.7.1.2)
- Awareness training on Information Security Policy, associated policies and other relevant statutory compliances shall be conducted by CISO on (Ref. A.7.2.2):
    - Induction of new employees, contractor or third party into the organization
    - On changes to the information security policies for all existing employees, contractors and third party.
- All the employees, contractors and third party shall comply and adhere to the CIPL's Information Security policy. (Ref. A.7.2.1)
- Any violation or non-compliance of Information Security Policy by Employee, contractor or third party shall call for formal disciplinary action. (Ref. A.7.2.3)
- After termination of services or internal transfer, employee, contractor or third party, shall abide by the Information Security policy in accordance with the NDA signed during recruitment or as per appointment letter. (Ref. A.7.3.1)

- In the event of termination; the employee, contractor or third party shall return all the organizations assets in their possession as per formal termination procedure. (Ref. A.8.1.4)
- In the event of change of role, the employee, contractor or third party, shall return all the organizations assets in their possession. (Ref. A.8.1.4)
- In the event of termination, the employee, contractor or third party's physical and logical access rights shall be revoked and if necessary transferred to designated person for monitoring purpose. (Ref. A.9.2.6)
- In the event of change of role; the employee, contractor or third party's physical and logical access controls shall be withdrawn that are not relevant to his new engagement / role and if necessary transferred to designated person for monitoring purpose. (Ref. A.9.2.6)

13.3 Communication of Policy Details

This policy and relevant specific policies, procedures shall be published on Company's Intranet and communicated to employees and relevant external parties.

13.4 Periodical Review

The information security policy shall be reviewed on yearly basis or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

The Information Security Management Forum would review this Policy, the compliance and implementation status, effectiveness of controls and their implementation, taking into account Internal Audit Reports, Incidents, suggestions and feedback from related parties and make appropriate recommendation for improvements.

13.5 Violation of the Information Security Policy

Non-compliance or violation of the CIPL's Information Security policy shall result in disciplinary action as per the CIPL's Human Resource Policy and other such rules prevalent at the time of violation.

13.6 ISO Controls

- A.6.1.1 Roles and responsibilities
- A.7.1.2 Screening
- A.7.1.2 Terms and conditions of employment
- A.7.2.1 Management responsibilities
- A.7.2.2 Information security awareness, education and training
- A.7.2.3 Disciplinary process
- A.7.3.1 Termination responsibilities
- A.8.1.4 Return of assets
- A.9.2.6 Removal of access rights

13.7 References

- Information Security Policy
- Human Resource Procedure

14. Acceptable Usage Policy – PO – 14

14.1 Purpose

This policy addresses the need to implement appropriate controls for the secure use of information systems resources in CIPL for business purposes.

14.2 Policy Details

This policy applies to all users of Information and IT resources in CIPL.

14.2.1 Policy Statement

Activities considered unacceptable and subject to disciplinary actions (PR-13 Human Resource Procedure) are as follows but not limited to:

- Employees not following the Information Security Policy while working with IT Infrastructure and accessing information of CIPL, using IT Infrastructure.
- Employees indulging in any activity that violates local, national and inter-national applicable laws and the Information Security Policy of CIPL during and after their tenure with CIPL. (Ref. A.18.1.1)
- Secret information gathering on or of the company's / company's client's assets. (Ref. A.18.1.4)
- Unauthorized copying of copyright material as mentioned below but not limited to (Ref. A.18.1.2):
- Digitization and distribution of photographs from magazines, books, etc. using CIPL's Infrastructure resources.
- Customer's Information.
- Software procured by company.
- Exporting software, technical information, encryption software or technology, documentation in violation of company policy or rule of the land.
- Leaving the equipment unattained without appropriate protection or security. (Ref.A.11.2.8)
- Leaving removable media, documents on desk unattended. (Ref.A.11.2.9)
- Introduction of malicious programs into the network or server (e.g. viruses, worms, Trojans, e-mail bombs, etc.).
- Revealing account password to others or allowing use of account by others including family and other household members when working from out of CIPL premises. (Ref.A.9.3.1)
- Making fraudulent offers of products, items or services originating from any CIPL account. (Ref. A.18.1.3)
- Effecting security breaches or disruptions of network communication include, but are not limited to, (For the purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service and forged routing information for malicious purposes.)
- Accessing data of which the user is not an intended recipient or logging into a server.
- Account that the user is not expressly authorized to access, unless these duties are within the scope of regular duties.
- Circumventing user authentication or security of any host, network or account.

- Unauthorized port scanning or security scanning.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program / script / command or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet / Intranet / Extranet.
- Providing information about, or lists of, CIPL employees to parties outside CIPL. (Ref.A.18.1.4)
- Attempt to test a suspected weakness in the environment without authority.
- Violation of Acceptable Usage Guidelines (Ref. A.8.1.3).

14.3 Communication of Policy Details

This policy and relevant specific policies, procedures shall be published on Company's Intranet and communicated to employees and relevant external parties.

14.4 Periodical Review

The information security policy shall be reviewed on yearly basis or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

The Information Security Management Forum would review this Policy, the compliance and implementation status, effectiveness of controls and their implementation, taking into account Internal Audit Reports, Incidents, suggestions and feedback from related parties and make appropriate recommendation for improvements.

14.5 Violation of the Information Security Policy

Non-compliance or violation of the CIPL's Information Security policy shall result in disciplinary action as per the CIPL's Human Resource Policy and other such rules prevalent at the time of violation.

14.6 ISO Controls

- A.8.1.3 Acceptable use of assets.
- A.9.3.1 Password use
- A.11.2.8 Unattended user equipment
- A.11.2.9 Clear desk and clear screen policy
- A.18.1.1 Identification of applicable legislation.
- A.18.1.2 Intellectual property rights (IPR).
- A.18.1.3 Protection of organizational records.
- A.18.1.4 Data protection and privacy of personal information.

14.7 References

- Information Security Policy
- Password Policy
- Human Resource Policy
- Human Resource Procedure
- Acceptable Usage Guidelines

15. Communication Policy – PO – 15

15.1 Purpose

This policy addresses business disruption due to improper usage of communication devices.

15.2 Policy Details

This policy applies to the use of all communication devices in CIPL.

15.2.1 Policy Statement

- Confidentiality and integrity of business interest information shall not be compromised through the improper use of communication devices. (Ref. A.6.2.2)
- Availability of critical communication devices shall be ensured at all times.
- The confidential and restricted documents shall not left behind on facsimile and coping devices.
- The confidentiality and integrity of business information shall be maintained while having verbal communication through telephonic network.
- Communication of highly critical business information shall be done in secure areas to prevent eavesdropping / overhearing. (Ref.A.6.2.2)
- Modem/Mobile phone usage (Ref.A.6.2.1)
    - Usage of modem / mobile phone along with personal computer or other communication devices shall be strictly prohibited.
    - Concession shall be granted to use modem with such devices and data network only with specific approval of Manager IT.
- Copier usage policy
    - After confidential documents have been copied user should make sure that no original or superfluous copies are left behind
    - Bad copies of confidential documents are also sensitive and should be destroyed at the earliest. (Ref.8.3.2)
    - It should be ensured that with double sided copying no copies remains behind the duplex trays.
    - Copies that have been left or forgotten in copier by others should be handed over to people concerned or destroyed. (Ref.A.11.2.9)

15.3 Communication of Policy Details

This policy and relevant specific policies, procedures shall be published on Company's Intranet and communicated to employees and relevant external parties.

15.4 Periodical Review

The information security policy shall be reviewed on yearly basis or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

The Information Security Management Forum would review this Policy, the compliance and implementation status, effectiveness of controls and their implementation, taking into account Internal Audit Reports, Incidents, suggestions and feedback from related parties and make appropriate recommendation for improvements.

15.5 Violation of the Information Security Policy

Non-compliance or violation of the CIPL's Information Security policy shall result in disciplinary action as per the CIPL's Human Resource Policy and other such rules prevalent at the time of violation.

15.6 ISO controls

- A.13.2.1 Information exchange policies and procedures
- A.11.2.9 Clear Desk and Clear Screen Policy
- A.6.2.1 Mobile Computing and Communications
- A.6.2.2 Tel-working
- A.8.2.3 Information Handling Procedures

15.7 References

- Information Security Policy
- Human Resource Policy

16. Email Policy – PO – 16

16.1 Purpose

The purpose of the policy is to

- Encourage an efficient communication system to add value to the services offered by CIPL.
- Implement adequate usage controls to ensure that the E-mail facility provided by CIPL is used only for the official purpose. E.g. content filtering, mail box size restrictions, mass mailing controls, E-mail usage logs, attachment size controls etc.
- Implement adequate security controls to ensure that the vulnerabilities associated with E-mail facility are minimized e.g. antivirus
- Educate the users about the applicability of this policy

16.2 Policy Details

The policy applies to:

- All E-mail systems and services provided or owned by CIPL.
- All Users of CIPL's E-mail services
- All E-mail records in possession of the employees or other use of other E-mail services through a gateway provided by CIPL.

16.2.1 Policy Statement

- The Electronic Mail facility provided by CIPL shall be used by the authorized users and only for official purpose. Users shall be responsible for the communications carried out through their user ID.
- To protect against the E-mail related vulnerabilities, security controls like anti-virus, content filtering and log monitoring shall be implemented.
- Ownership
    - IT Manager shall be the Owner and shall maintain the infrastructure and its security thereof as per the Network Policy.
- Authorization / Assignment
    - Project Manager working as Mail Administrator after obtaining approval from IT Manager shall assign E-mail access.
    - E-mail access shall be assigned as per the Access Control Policy and the Password Policy.
    - Each user shall be responsible for any activity performed through his / her E-mail ID.

16.2.2 Access Control

Users shall be identified and authenticated at the network level before allowing access to the E-mail facility wherever supported, E–mail users shall be again identified and authenticated at the E-mail application software level.

Specific Provisions for Use of E-mail:

- **Restrictions:**
  CIPL's E-mail services shall not be used for: any unlawful activities, personal financial gain, any other use that violates other policy and guidelines for CIPL regarding intellectual property, or any form of harassment. Transmission / Re-transmission of unofficial chain messages are prohibited. The E-mail facility is CIPL's property. Without any prior notice CIPL has a right to examine, copy, and stop or delete any E-mails including personal folder, of any employees. CIPL may disclose any E-mail messages sent or received by any employee, to law enforcement authorities without any prior notice to the employee.

  However, such monitoring activity or disclosures shall be authorized by the Owner or any other appropriate business head.

- **Size of Mail Box for each User shall be minimum 200MB.**
- **E-mail Attachments:**
  To prevent computer viruses, employees shall not open e-mail attachments that are from an unknown or entrusted source. Employees are expressly prohibited from creating or sending computer viruses through E-Mail. When sending E-Mails with attachments, all attachments shall as far as possible be zipped.
- **Attachment size restriction:**
  The size of an E-mail shall not be more than 5MB when sent to an individual / groups outside CIPL and not more than 5MB when sent to an individual / groups within CIPL.
- **Representation:**
  E-mail users shall not give the impression that they are representing, or otherwise making statements on behalf of CIPL unless appropriately authorized to do so.
- **False Identity:**
  E-mail users shall not employ false identity or send anonymous E-mails.
- **Interference:**
  CIPL's E-mail services shall not be used for the purposes that could cause, directly or indirectly, excessive strain on the computing facilities of CIPL or interference with the others' use of the E-mail services
- **Personal Use:**
  CIPL's E-mail services may be used for incidental personal purposes provided that:
    - it is not for personal financial gain
    - it does not cause strain on the computing facilities of CIPL;
    - burden the CIPL with noticeable incremental cost;
    - Interfere with the E-mail user's duties and responsibilities to the CIPL.
- **Reporting:**
  Employees shall report offensive E-mails to their Helpdesk. The same shall be escalated to the Owner.

16.2.3 Security and Confidentiality

- All incoming e-mails shall be scanned for viruses as per CIPL's Virus Policy.
- User shall be informed to exercise caution in using E-mail to communicate confidential or sensitive matters.
- Users of E-mail services shall be informed that during the performance of their duties, personnel may view the contents of the E-mail. However, the personnel shall not disclose / use the contents thereof for any purpose.

- Users of E-mail services shall be aware that even though the sender and the receiver may have discarded their copies of the E-mail record, there may be backup copies in CIPL archive that may be retrieved.
- Users shall not employ a scanned version of a hand-rendered signature to give the impression that an E-mail message was signed by the sender as the signature could be misused by another person.
- Using another individual's E-mail account is strictly prohibited except in the following cases:
    - In case a user is on leave and there is a need to read E-mails in his / her mailbox. Such access shall be permitted after obtaining an authorization.
    - Secretaries may have access to the mailbox of the head.
    - Generic IDs (project IDs or helpdesk IDs etc.) created under proper authorization and allowed to be accessed by the relevant team members
- In all these cases "read / receive only" access shall be given and sending mails through such Ids shall be prohibited.
- Automatic forwarding of E-mail
    - Users shall not automatically forward their e-mails to any address outside the group / company networks

16.2.4 Protection of e-mails due for legal purposes

- Whenever a legal notice is received or an authorized person so directs, the identified e-mails and logs shall be preserved for the necessary period.
- Wilful access to and use of the assigned IDs shall be prohibited.

16.3 Communication of Policy Details

This policy and relevant specific policies, procedures shall be published on Company's Intranet and communicated to employees and relevant external parties.

16.4 Periodical Review

The information security policy shall be reviewed on yearly basis or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

The Information Security Management Forum would review this Policy, the compliance and implementation status, effectiveness of controls and their implementation, taking into account Internal Audit Reports, Incidents, suggestions and feedback from related parties and make appropriate recommendation for improvements.

16.5 Violation of the Information Security Policy

Non-compliance or violation of the CIPL's Information Security policy shall result in disciplinary action as per the CIPL's Human Resource Policy and other such rules prevalent at the time of violation.

16.6 ISO controls

- A.13.2.1 – Information transfer policy and procedure

16.7 References

- Password Policy
- Human Resource Policy
- Network Policy
- Anti-Virus Policy
- Information Backup Policy

17. Network Management Policy – PO – 17

17.1 Purpose

The purpose of this policy is

- To ensure secure flow of the information through the network with implementation of appropriate controls for confidentiality, integrity and availability of information.
- To maintain confidentiality, integrity and availability of CIPL's information assets
- To implement effective access controls to prevent unauthorized access

17.2 Policy Details

This policy applies to

- The Information in CIPL network assets
- Various network components such as Data cables, hubs, switches, patch panels, routers, firewall, Network management system, Intrusion detection system, File integrity system network log analysis system.
- All users including network administration, system administration, vendors and vendors staff, maintenance staff and contractors of CIPL network assets

17.2.1 Ownership

The IT Manager shall be owner of the policy and the network infrastructure and shall be responsible for the maintenance of the integrity and availability of CIPL network.

17.2.2 Network management

- CIPL network shall be segregated from external network by appropriate controls like network design, routing controls and intrusion detection system
- CIPL shall implement appropriate network management and diagnostic tools to monitor the security and health of the network
- All network assets and network management tools shall be configured in accordance with best practices

17.2.3 Network Inventory

- The owner shall maintain an inventory of all network components and classify the same as per the Risk Management Policy
- Up-to-date network diagram shall be maintained at all times
- Any changes to the network design and components shall be carried out as per the Change Management Policy
- All network assets shall be physically protected as per the Physical and Environmental policy of the CIPL.
- All network assets shall be logically secured and configured in accordance with the vendors advices and best practices
- CIPL network shall be secured from outside networks, internet and third party networks

- Access to network management and diagnostic tools shall be provided to authorized users only
- Access for users to the network shall be as per Password Policy
- Access for external users shall be granted only after carrying out a formal risk assessment and shall be as per the Password Policy
- Interconnection between CIPL and Third party network shall be implemented only after carrying out a formal risk assessment and authorization.

17.2.4 Communication

- Data passing through the network shall be classified as per the Asset Classification and Handling policy. Data classified as "Highly critical" shall be transmitted through an encrypted channel and proper security measures shall be enforced.
- Remote access to CIPL network shall be permitted only after authorization from the Owner / IT Manager and after adequate security measures such as (two factor authentication and RSA Key) are enforced for the same.
- External users shall be permitted to remotely log into CIPL network to provide maintenance and support services only after proper approval from Owner / IT Manager and adequate security measures such as (two factor authentications and RSA Key) are enforced for the same.

17.2.5 Monitoring

- Audit trail logs shall be generated for all network assets
- Appropriate date and time stamping controls shall be implemented to ensure accuracy and analysis of network logs.
- Network Time synchronization server shall be used to synchronize timings of all network equipment.
- All network resources, services, access and their usage shall be monitored by the network owner
- All traffic through the gateways shall be monitored for possible misuse and intrusion.
- Intrusion detection system (IDS) logs shall be reviewed for malicious activities.

17.2.6 Change of Password

- Where applicable, all default passwords for access to various network devices shall be changed before moving to the production environment.
- All network services shall be controlled.
- Only those services which are necessary for CIPL Business shall be enabled.

17.2.7 Remote Access Requirements for Entities

- External users shall be permitted to remotely log into CIPL network only after proper approval from Owner / IT Manager and adequate security measures such as (two factor authentications and RSA Key).
- Although the remote access may be pre-approved, CIPL reserves the right to terminate or revoke this ability at any time for any entity.

- Any exceptions for providing remote access to an entity that do not meet the requirements stated in this policy or by a means not via the current infrastructure must be communicated to the IT Manager for review prior to implementation.

17.2.8 Wide Area Network Considerations

This connection is based on a negotiated contract with a service provider that was determined by the IT Manager. This contract is based on a broad consideration of the business needs. Since a service provider is responsible for this connection, responsibilities must be delegated in case of issues with this connection.

17.2.8.1 Wide Area Network Incident Reporting

It is the responsibility of the local IT Team to report any incidents or outages with their Wide Area Network connection. This means for opening a ticket has been authorized to certain individuals at the IT Team. The local IT teams are not responsible for opening up an incident for local unit connection issues.

Any questions related to the incident management process or to obtain access to the ticketing system can be directed to the local IT Team.

17.2.8.2 Resolution Escalation

In the event that an incident is not solved in a timely manner or whose resolution deadline has been exceeded, the local IT Team shall contact the IT Team with the issue and include the incident number with this communication. The local IT Team shall assess and escalate the issue to their contacts at the service provider.

17.2.9 Wide Area Network Terms of Use

The Wide Area Network connection is a critical means for communication within CIPL. In order to preserve this communication it is necessary to establish some terms of use.

17.2.9.1 Refusal of Service

CIPL Corporate IT has the right to refuse or limit service to any country unit at any time. Although unlikely, reasons for refusal of service may include the following:

- To prevent or limit the local unit's exposure to a malicious attack that may be impacting the rest of the network.
- To block a malicious attack coming from the local IT unit that has the potential to impact the rest of the network.

17.2.9.2 Reporting of On-going Issues

In the case that the local unit is dissatisfied with the level of service of their Wide Area Network connection due to concerns that the business needs are not being met, the unit may contact the IT Team. These issues may be brought up to the service provider and also be taken into consideration for future evaluation purposes.

17.2.10 Local Area Network

CIPL expects its Country Unit to only have their Local Area Network connected to the Wide Area Network. The Local Area Network cannot be extended to any other networks. Local Internet In- and Outbound connections are not permitted. Any exceptions to this rule require prior approval by the IT Manager. Approval can be obtained by reporting the connection to the IT Team personnel along with the business case.

17.2.10.1 Local Area Network IP Addressing

CIPL provides its subsidiaries with a range of private IP addresses. These can be used at the subsidiary's discretion. No other IP address ranges except for those designated to the subsidiary are allowed on the CIPL Network. Please defer all questions to the local IT hub team.

17.2.10.2 Local Area Network Design

The Local Area Network can be designed by the subsidiary; however, it is strongly recommended that the design meet the guidelines and requirements from the CIPL Global LAN Design Guideline.

17.2.10.3 Local Area Network Security

Local Area Network Security devices, such as routers, content filters, and proxy URLs can only be placed into production when authorized by the IT Team. The IT Team personnel reserve the right to inspect the configuration of these devices.

17.2.10.4 Local Area Network Connection Reporting

Each unit must report the status of any existing in or outbound connections not managed by Corporate IT on an annual basis, regardless of whether the connection has been previously approved. The connections will be reviewed for re-approval.

17.2.11 Wireless Local Area Network

The Wireless Local Area Network is an extension of the Local Area Network. By nature, the Wireless Local Area Network is harder to confine to a specific area and also the integrity of the connection may not be as robust as a wired connection. Special rules apply to the Wireless Local Area Network (WLAN).

17.2.11.1 Acceptable Wireless Local Area Networks

CIPL Corporate IT provides an approved wireless solution. This covers all security aspects and guarantees consistency for non-wired connections throughout the organization. It is forbidden to extend the Local Area Network with any kind of wireless transmitting device which has been Corporate IT approved. Such devices include:

- Wireless Access Points

17.2.11.2 Wireless Local Area Network Equipment

CIPL Corporate IT provides the appropriate equipment to establish the Wireless Local Area Network.

17.2.12 Computers used to connect to the Local Area Network

The entity's equipment must meet certain requirements prior to connecting to the Local Area Network. The equipment must meet the following:

- The equipment is a CIPL managed computer, or
  - A non-CIPL computer inspected by a qualified local CIPL IT department to ensure all of the following points are met
  - The equipment is owned and handled by a pre-authorized entity who has an agreement with CIPL which addresses the following points
    - The Operating System and other software loaded on it must be current on patches within 1 month or earlier to prevent exposure to CIPL's resources from vulnerabilities or other potentially malicious threats
    - Must have a functioning anti-virus client installed with current virus definitions
    - Is compatible with any software used to facilitate the remote access without compromising the integrity or confidentiality of the connection
    - Is configured in such a way as to prevent the bridging of local network connections

17.3 Communication of Policy Details

This policy and relevant specific policies, procedures shall be published on Company's Intranet and communicated to employees and relevant external parties.

17.4 Periodical Review

The information security policy shall be reviewed on yearly basis or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

The Information Security Management Forum would review this Policy, the compliance and implementation status, effectiveness of controls and their implementation, taking into account Internal Audit Reports, Incidents, suggestions and feedback from related parties and make appropriate recommendation for improvements.

17.5 Violation of the Information Security Policy

Non-compliance or violation of the CIPL's Information Security policy shall result in disciplinary action as per the CIPL's Human Resource Policy and other such rules prevalent at the time of violation.

17.6 ISO Controls

- A.12.1.1 Network controls
- A.13.1.2 Security of Network services

17.7 References

- Risk Management Policy
- Physical and Environmental Policy
- Password Policy
- Change Management Policy

18. Internet Policy – PO – 18

18.1 Purpose

The purpose of the policy is to

- Implement adequate usage controls to ensure that the facility provided by CIPL is used only for appropriate official purpose.
- Implement adequate security controls to ensure that the vulnerabilities associated with the Internet are minimized e.g. antivirus.
- Educate the users about the applicability of this policy

18.2 Policy Details

The policy applies to:

- All systems and services provided or owned by CIPL for the Internet connectivity.
- All Users of CIPL's Internet services.

18.2.1 Ownership

- Manager IT shall be the Owner of the Internet infrastructure.

18.2.2 Authorization

- Internet access shall be provided by the Owner or after obtaining a request from the authorized person through Service Now Tool.

18.2.3 Access Control

- Users shall be identified and authenticated at the network level before allowing access to the Internet facility.
- User access to the Internet shall be through AD Access to ensure that the appropriate control measures can be implemented e.g. logging of the user activities, access and content filtering, hiding the internal IP addressing scheme etc.
- Users shall not connect to the Internet except through the approved resources provided by the CIPL. Any attempt to connect to the Internet through the non-approved resources is strictly prohibited.

18.2.4 Access and Content Filtering

- Appropriate content / access filtering technology shall be implemented to prevent the users from accessing inappropriate sites.

18.2.5 Antivirus Implementation

- User access to the Internet shall be scanned for virus infection through an automatic anti-virus scanning mechanism at the internet gateway

18.2.6 Logging of Internet Usage

- Adequate and secure audit trails of Internet access shall be generated to ensure accountability and monitor access violations. The Internet facility is CIPL's property and shall be monitored without any prior notice.

18.2.7 Internet Usage Code of Conduct:

- Each user is responsible for the activities carried out through his / her user ID.
- Ability to connect to a specific web site does not in itself imply that users of CIPL's Internet facility are permitted to visit that site. Users using CIPL's Internet facility shall immediately disconnect on discovering that they are connected to a potentially offensive site.
- CIPL's Internet services shall be used for official purposes. These resources shall not be used for any unlawful or prohibited activities like hacking, gambling, accessing CIPL's restricted / confidential data or any other use that violates any law or policy of the CIPL.
- CIPL's Internet services shall not be used for the purposes that could cause, directly or indirectly, excessive strain on the computing facilities of the CIPL or interference with use of Internet services by other users. Such interference may be terminated manually / automatically.

18.2.8 Personal Use

CIPL's Internet services may be used for incidental personal purposes provided that:

- it is not used for personal financial gain;
- it does not cause strain on the computing facilities of the CIPL;
- burden CIPL with noticeable incremental cost;
- Interfere with the User's duties and responsibilities to CIPL.

18.2.9 User Awareness

- All users shall be adequately made aware about CIPL's policy on the Internet usage.

18.3 Communication of Policy Details

This policy and relevant specific policies, procedures shall be published on Company's Intranet and communicated to employees and relevant external parties.

18.4 Periodical Review

The information security policy shall be reviewed on yearly basis or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

The Information Security Management Forum would review this Policy, the compliance and implementation status, effectiveness of controls and their implementation, taking into account Internal Audit Reports, Incidents, suggestions and feedback from related parties and make appropriate recommendation for improvements.

18.5 Violation of the Information Security Policy

Non-compliance or violation of the CIPL's Information Security policy shall result in disciplinary action as per the CIPL's Human Resource Policy and other such rules prevalent at the time of violation.

18.6 ISO controls

- A.13.2.1 Information exchange policies and procedures

18.7 References

- Password Policy
- Network Policy
- Anti-Virus Policy

19. Anti-Virus Policy – PO – 19

19.1 Purpose

The purpose of the policy is to ensure that

- To protect CIPL's information assets from malicious codes, like worms and viruses.
- To avoid loss of / damage to CIPL's information assets caused due to malicious software like viruses and worms.
- To keep the antivirus software up-to-date with latest signatures
- Educate the users about the applicability of this policy.

"To ensure that CIPL's information assets are protected against malicious codes, like viruses and worms, appropriate security and control procedures shall be implemented."

19.2 Policy Details

The policy applies to:

- All the servers, Desktops and laptops used within CIPL
- All Desktop, Email, Internet and other information system users

19.2.1 Ownership

Manager IT shall be the Owner and shall be responsible for the implementation, maintenance and review of the policy.

19.2.2 Anti-Virus Management

- The Owner shall monitor all virus incidents to ensure that they can be traced back to the location within CIPL.

- The anti-virus servers shall be continuously updated with the latest versions of the virus definition files. The antivirus server shall push the updated definitions to the laptops, desktops and other servers
- Desktops and laptops shall be scanned. Bypassing of the in-built scanning process shall be strictly prohibited
- The Business Owner shall approve all changes to the anti-virus configuration as per Change Management Policy.
- Access to USB drives shall be prohibited unless authorized by the Business Owner.

19.2.3 Acceptable Usage

- All files downloaded from e-mail attachments, copied from CDs or by file-sharing etc. shall be scanned for viruses. (A.15.1.2)

19.3 Communication of Policy Details

This policy and relevant specific policies, procedures shall be published on Company's Intranet and communicated to employees and relevant external parties.

19.4 Periodical Review

The information security policy shall be reviewed on yearly basis or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

The Information Security Management Forum would review this Policy, the compliance and implementation status, effectiveness of controls and their implementation, taking into account Internal Audit Reports, Incidents, suggestions and feedback from related parties and make appropriate recommendation for improvements.

19.5 Violation of the Information Security Policy

Non-compliance or violation of the CIPL's Information Security policy shall result in disciplinary action as per the CIPL's Human Resource Policy and other such rules prevalent at the time of violation.

19.6 ISO controls

- A.15.1.2 Addressing security in third party agreements
- A.12.2.1 Control against Malicious code

19.7 References

- Email policy
- Network Policy
- Internet Policy
- Change Management Policy

20. Mobile Computing Devices Security Policy – PO – 20

20.1 Purpose

This policy addresses secured usage of mobile computing devices in CIPL.

20.2 Policy Details

The policy applies to:

- This policy applies to all users of mobile computing devices in CIPL.

Mobile computing devices imply but are not limited to:

- Laptops / Notebooks
- USB/ Zip/ Pen/ Flash Drive
- CD writers
- HDD/Web cam
- Smart Phones
- Digital Camera
- Tape and Cartridges Devices

20.2.1 Policy Statement

- Visitors / non-employees shall be allowed to carry mobile computing devices inside the premises in accordance with the requirements of the same devices.
- All the mobile computing devices shall adhere to policy and procedure defined to take care of Mobile computing devices used in CIPL, with prior permission.
- Prior approval from Manager IT shall be required to carry mobile computing devices in CIPL.
- CIPL employees shall be eligible to use mobile computing devices based on role, designation and approval by the Concerned Department Head and shall return the assets immediately after transfer or separation from CIPL. (Ref.7.3.1)
- Highly Critical / confidential information shall be protected when stored on mobile computing devices. (Ref. 8.2.3)
- Mobile computing devices shall not connect to Internet directly when they are connected to any of the CIPL Network.
- Hardware / Software configuration changes of any mobile computing device shall adhere with the Change Management Policy.
- Contract employees and Third party's Mobile devices shall not be connected to CIPL network without approval from Manager IT.
- For specific case the permission shall be granted from Concerned Network Owner, for connecting to CIPL Network and providing access right to CIPL information. This shall be executed through Change Management Procedure. (Ref.A.6.2.1)
- The person carrying out change management shall ensure that the mobile device shall be tested for malicious code.
- Access to information on mobile computing devices or through CIPL Network shall adhere to Physical and Environmental Policy and Access Control Policy - Logical.

- Wireless Network shall be allowed to use Notebooks / Smart Phones only for employees
- Wireless Network shall be allowed for any visitors or third party team members

20.3 Communication of Policy Details

This policy and relevant specific policies, procedures shall be published on Company's Intranet and communicated to employees and relevant external parties.

20.4 Periodical Review

The information security policy shall be reviewed on yearly basis or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

The Information Security Management Forum would review this Policy, the compliance and implementation status, effectiveness of controls and their implementation, taking into account Internal Audit Reports, Incidents, suggestions and feedback from related parties and make appropriate recommendation for improvements.

20.5 Violation of the Information Security Policy

Non-compliance or violation of the CIPL's Information Security policy shall result in disciplinary action as per the CIPL's Human Resource Policy and other such rules prevalent at the time of violation.

20.6 ISO controls

- A.8.1.4 Return of assets
- A.8.2.3 Information handling procedures
- A.6.2.1 Mobile computing and communications.

20.7 References

- Information Security Policy
- Access Control Policy – Logical
- Physical and Environmental Policy
- Acceptable Usage Policy
- Anti-Virus Policy
- Change Management Policy
- Mobile Computing Devices Security Procedure

21. Backup Policy – PO – 21

21.1 Purpose

This policy addresses backup policy to be implemented for CIPL.

- To ensure that backups of all the identified highly critical information assets are taken and are tested for readability / restoration at regular intervals.
- To ensure that backups are stored for adequate period as per CIPL's Data Retention Policy.
- To ensure that adequate sets of backups (at least two) are taken for all highly critical information assets and at least one set is stored at the identified off-site locations.
- To ensure that all backups are labelled, inventoried, and movement between onsite and offsite locations are recorded,
- To ensure that media stored is physically and environmentally secured.
- To ensure that a location-wise inventory is maintained for the new backed up and out of use media (identified for destruction).
- To ensure that the backup media is taken out of recycling after the vendor specified number of writes or after encountering any error.

    - To ensure availability of the information, adequate backups of the operating systems, applications, databases, network configurations, and identified personal computers, shall be taken and retained.
    - The backup media shall be stored in safe and secure environment.
    - Adequate security procedures shall be implemented to ensure that the media in transit is traceable and secured against loss, damage or theft.

21.2 Policy Details

The policy applies to:

- Backup process for servers, applications, databases, network components, and identified personal computers at CIPL
- Labelling, storage, handling and movement of backup media.
- Testing and restoration of the backup media.
- Recycling and destruction of the backup media.

21.2.1 Responsibilities of Defining Backups

Owners of the information assets like operating systems, databases, applications, network components and other information assets shall identify the data to be backed up.

The information asset owners shall decide appropriate backup plan, taking into consideration its importance to the CIPL's business, legal requirements and technology available.

The owners of information assets, in consultation with the IT dept., shall prepare a backup schedule. The backup schedule shall consist of details like:

- Responsibility of taking backup as per the backup schedule
- List of directories and files to be backed up
- Type of media - LTO
- Timing of start and completion of backup
- Number of copies
- Storage locations
- Backup application (e.g. Symantec tool)
- Rotation and archival schedule
- Testing and restoration frequency and procedures
- Retention period

21.2.2 Responsibilities of Taking Backups

The identified owner, on behalf of the Manager IT/CISO, shall be made accountable for taking backups of the information assets at the Data Centre. Backup of all critical information on individual desktops shall be taken by the user of desktop itself.

21.2.3 Documentation and Records

- The backup plan with a schedule shall be documented and shall be available for reference and verification with the information asset owner and the team responsible for the execution of the backup schedule.
- The backup plan shall also identify the reporting procedures for the execution of the backup schedule and problems encountered.
- Wherever possible automated audit trails shall be generated for the backup activity and exceptions shall be reported to the information owner.

21.2.4 Inventory of Backup media:

A complete inventory shall be maintained of

- The media used for backups
- Unused media (blank)

21.2.5 Choice of Backup media and Backup application:

Choice of backup media shall be guided by considerations like

- size of data to be backed up
- requirements of backup application
- speed of backup and restoration process
- data retention requirement
- the expected life of storage media itself
- reliability requirements
- available technology

21.2.6 Rotation/recycling of backup media:

Backup media shall be rotated ensuring that

- Adequate generations of backups are available.
- The media is not recycled (reused for taking backups) beyond 'number of writes' as prescribed by the vendor of the media.

21.2.7 Storage of Backup media:

- At least one full latest backup set shall be stored offsite.
- All backups (on site and off site) shall be stored in secure locations in a controlled environment as per Physical and Environmental Policy.
- A record of the storage of backups (on site and off site) shall be maintained.
- Backed up tapes shall be stored in specially identified fire resistant cabinets.

21.2.8 Media identification / labeling:

Media labeling shall help identify

- the contents
- date and time of backup
- Sequential number of the media
- The number of times the media has been used/reused

21.2.9 Media in transit:

- Backup media shall be transported in secured way
- Movement of media to and from the off site location shall be recorded in such a manner that each media is traceable
- Movement of media shall be authorized by the information owner
- Movement of media shall be carried out only by the identified person or through the identified agency.

21.2.10 Testing of the backup media for readability / restorability:

- Backed up media shall be tested for readability and restorability at regular intervals. The intervals for such testing shall be as per the backup plans prepared by the information owner.
- The results of such media health checks shall be documented and exceptions shall be reported and monitored.

21.2.11 Testing complete restorability/recoverability:

While carrying out a full restoration / recovery following things shall be considered

- Convenient timing of the test restoration / recovery
- Restoration shall be carried out only in a test environment.
- Restoration shall be possible only for those files which are selected
- Restoration shall be possible with the original (as in production) set of directory and file permissions
- Shall be witnessed by Information Owner.
- The Information Owner shall document the test results.

- If any problems are encountered during test restoration, then the backup plan / procedures shall be suitably modified. The modified / revised test restoration / recovery shall be scheduled immediately to confirm that the restoration occurs as desired.
- After the test restoration / recovery is complete, the restored data shall be removed

21.2.12 Technology Obsolesce:

- The Technology Department shall monitor the validity of the technology used for creating and maintaining backups. In case of any obsolescence in the existing technology, all backups, recorded in the existing, media shall be transferred using the upgraded technology by the Owner as per Change Management Policy.
- A record of such upgrades shall be maintained by the Owner

21.2.13 Destruction of Used/ Damaged Media

Wherever necessary the backup media shall be destroyed as per Disposal of Electronic Media and Computing Devices policy

21.3 Communication of Policy Details

This policy and relevant specific policies, procedures shall be published on Company's Intranet and communicated to employees and relevant external parties.

21.4 Periodical Review

The information security policy shall be reviewed on yearly basis or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

The Information Security Management Forum would review this Policy, the compliance and implementation status, effectiveness of controls and their implementation, taking into account Internal Audit Reports, Incidents, suggestions and feedback from related parties and make appropriate recommendation for improvements.

21.5 Violation of the Information Security Policy

Non-compliance or violation of the CIPL's Information Security policy shall result in disciplinary action as per the CIPL's Human Resource Policy and other such rules prevalent at the time of violation.

21.6 ISO controls

- A.12.3.1 Information Backup-up

21.7 References

- Information Security Policy
- Physical and Environmental Policy
- Disposal of Electronic Media and Computing Devices policy
- Change Management Policy

22. Patch Management Policy – PO – 22

22.1 Purpose

This policy defines the patch management for Operating system, Database and applications installed and configured on all servers, desktops systems, laptops and network devices in CIPL

22.2 Policy Details

22.2.1 Scope

This policy shall be applicable to

- All the operating systems including virtual
- All Network operating system
- Applications installed on servers, desktops, laptops and network devices connected in CIPL

22.2.2 Policy Statement

- Each operating system shall be updated with all concerned operating systems security patches in times manner and on regular basis.
- Each application installed on servers connected in CIPL should be updated with all latest patches available with specific vendor of the application through Change Management Procedure
- Each Network operating system installed on network devices like router, switch , firewall and IDS shall be updated with latest and stable patches
- New patches shall be reviewed and evaluated for relevance and criticality to the organization
- Consideration of non-applicability of the patch should be verified
- Patch management procedure and guidelines shall be observed during deployment of the patches
- All patches shall be appropriately tested before deployment of production system. In situations where available, system administrators shall automate the installation of Patch management, Usage of these tools assists in the uniform application of configurations, policies and patches at an enterprise wide level. If by using automated system, it was not possible to deploy patch on a particular server or desktop, automated system shall generate report stating exceptions.
- The technology Departments shall ensure deployments of latest vulnerability and security patches in IT environments
- Critical patches having active exploits shall be installed on priority basis.
- Non-critical patches shall be installed during schedules maintenance
- All networked devices belonging to or managed by IT departments will be patched with vendor provided system security patches.

22.3 Communication of Policy Details

This policy and relevant specific policies, procedures shall be published on Company's Intranet and communicated to employees and relevant external parties.

22.4 Periodical Review

The information security policy shall be reviewed on yearly basis or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

The Information Security Management Forum would review this Policy, the compliance and implementation status, effectiveness of controls and their implementation, taking into account Internal Audit Reports, Incidents, suggestions and feedback from related parties and make appropriate recommendation for improvements.

22.5 Violation of the Information Security Policy

Non-compliance or violation of the CIPL's Information Security policy shall result in disciplinary action as per the CIPL's Human Resource Policy and other such rules prevalent at the time of violation.

22.6 ISO controls

- A.14.2.9 – System acceptance
- A.12.5.1 – Control of operational software
- A.14.2.2 – Change control procedure
- A.12.6.1 – Control of Technical Vulnerability

22.7 References

- Patch Management Procedure
- Change Management Procedure

23. Change Management Policy – PO – 23

23.1 Purpose

The purpose of this policy is:

- to ensure a high level of integrity and correctness of information assets.
- to manage and control changes to the information assets
- to ensure that changes are documented and effectively reported
- to manage technology obsolescence

"The CIPL shall establish a framework for managing, controlling, documenting and reporting modifications to the information assets to ensure against unauthorized modifications."

23.2 Policy Details

The policy applies to:

- all employees, contractors, consultants, temporary users and third party employees who require access to the CIPL's information systems assets
- all changes, upgrades, or modifications to the information assets

23.2.1 Ownership

- The information asset owner shall be responsible for the implementation of the policy and plan the management of the asset.
- The Owner shall design and implement an appropriate Change Request process, with due approval wherever necessary, to ensure that change requests are evaluated, authorized, tested, documented and movement to production environment is controlled.(A.14.2.9)

23.2.2 Change Request

Any authorized person who controls part of the infrastructure, including all applications may submit a change request to the Owner (as per the procedure defined by the owner) or the Owner may initiate a change request, specifying the following:

- Date and Time
- Name and Designation of Person
- Name of the Information System Asset
- Change Requested By
- Problem encountered
- Requested change to mitigate the problem
- List of document(s) attached to substantiate change
- The Owner shall transfer the change request details to the Change Request Form
- Additionally, the Owner shall specify if the requested change is recommended / not recommended

23.2.3 Change Initiation and Approval

For a recommended change the Owner shall, after due study and evaluation, document a Change Request, which shall include the following:

- Change Description – a brief description of the change required
- Objective – the reason for making the change
- Affected Customers (internal, external or both)
- Priority – Low, High, Immediate
- Impact analysis - applications, end users, network segments, systems or business functions that would be affected by the change
- Threats – document potential failures
- Resource Requirement
- Responsibilities – personnel involved in making the change, User Acceptance Tests (before and after implementation of the change), and migrating the change to the production site
- Rollback Methodology
- Target dates - Probable Dates of testing and implementing the change in production environment.

The Owner, after preparation of the above documentation, shall seek the clearance of the Chief Information Security Officer who shall evaluate the request

- For its completeness, planning, rollback plans, the timing of the change such as year-end accounting etc.
- On obtaining a clearance from the Chief Information Security Officer, the Owner shall submit the Change Request documentation to the DC In-charge who shall execute the change.

23.2.4 Changes in change request form:

- Once a change request is accepted and approved, the Owner shall not make any changes to the original Change Request.
- If a need arises to make modification to the approved Change Request Form, the Owner shall inform all users involved in the process about the modifications. The original Change Request shall remain cancelled and a new Change Request shall be initiated.

23.2.5 The change Process

- The Owner and the IT Manager shall, identify the personnel who shall undertake the development of the change.
- The Owner shall identify personnel from the User group to carry out the User Acceptance Tests (UATs)
- The Owner shall submit the Change Request Documentation to the IT Manager to carry out the change
- The IT Manager shall be responsible for introducing the change and DC in-charge for maintaining all relevant documentation pertaining to the changes to the information assets.

23.2.6 Pre-implementation process:

The Owner shall review the change documentation submitted by the Technology Department:

- Test Plans—has there been adequate testing prior to determining outcomes
- Assurance from the personnel responsible for the change that only the changes as specified in the Change Request Form have been initiated and that the change shall not affect the functionality of other components
- Other dependencies—have they been completed (user training, documentation, user management etc.)
- Impact of the change on other scheduled / pending changes
- Backup of the existing system if required

The Owner shall submit the documentation to the Chief Information Security Officer, who shall ensure that the documentation is complete and security of the information assets is maintained. The Chief Information Security Officer shall submit a clearance, along with all documentation, for the implementation of the change

23.2.7 Change Implementation Process:

On receipt of a clearance from the Chief Information Security Officer, the Owner shall request the IT Manager to implement the change ensuring that there exists a separation of duties between the personnel who developed the change to the information assets and the personnel who would be moving the changes to the production environment.

23.2.8 Post- implementation process:

The owner shall monitor and submit a report stating the success / failure of the implementation of the change.
On report of a failure, the Owner shall initiate the rollback plan, if necessary. To reinitiate the change process, the Owner shall prepare a new Change Request.
On report of a success, the Owner shall

- maintain the modified version of the software in the library
- Inform the affected users about the implementation of the change along with training (if required) and all information (change in documentation / practice…etc.) pertaining to the change.

23.2.9 Emergency Change:

The Owner may undertake emergency changes, if necessary, to recover from a system failure, hardware problems or application problems.

Documentation of an emergency change shall include:

- Name of the user who reported the problem & the probable reason of interruption in service
- Name of the user who has carried out the emergency change.
- Date-time of the emergency change.
- An emergency work around until the problem is finally resolved
- The period of time till this workaround may be continued
- The risks involved in the workaround and the minimum security requirements to address these risks

A ratification of the emergency change as per the Change Request procedure shall be obtained by the owner at the first available opportunity.

23.3 Communication of Policy Details

This policy and relevant specific policies, procedures shall be published on Company's Intranet and communicated to employees and relevant external parties.

23.4 Periodical Review

The information security policy shall be reviewed on yearly basis or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

The Information Security Management Forum would review this Policy, the compliance and implementation status, effectiveness of controls and their implementation, taking into account Internal Audit Reports, Incidents, suggestions and feedback from related parties and make appropriate recommendation for improvements.

23.5 Violation of the Information Security Policy

Non-compliance or violation of the CIPL's Information Security policy shall result in disciplinary action as per the CIPL's Human Resource Policy and other such rules prevalent at the time of violation.

23.6 ISO controls

- A.12.1.2 Change Management
- A.14.2.9 System acceptance.

23.7 References

- Information Security Policy

24. Desktop Policy – PO – 24

24.1 Purpose

The purpose of this policy is:

- To minimize the loss of data or Desktop failure due to malicious software like viruses and worms
- To prevent unauthorized access to Desktops and the data residing on it.
- Implement adequate usage controls to ensure that the facility provided by CIPL is used only for appropriate official purpose
- Educate the users about the applicability of this policy.

"All the Desktop computers used within CIPL shall be used by authorized users for official purpose only, and shall be protected from unauthorized access, theft, data loss, viruses and other threats related to computing environment."

24.2 Policy Details

The policy applies to:

- All the Desktops owned by and used within the CIPL
- All Desktop Users

24.2.1 Ownership

The Department Head shall be responsible to maintain the security and availability of the Desktops.

24.2.2 Access Control

- Desktops shall be provided after obtaining a request from the Department Head.
- Each Desktop shall be identified and authenticated at the server level (e.g. Active Directory)
- Desktop access shall be assigned as per request from Department Head
- Each user shall be responsible for the applications or services used through his / her User Id
- Access to application software shall be provided as per request from Department Head
- Desktop utilities shall be restricted on a “need to know” and “need to do” basis.

24.2.3 Minimum Security Standard:

- Ensure that boot sequence for all Desktops is hard disk first.
- Floppy drives, CD-ROM and USB drives shall be disabled from desktops and will be enabled on need to do basis.
- Modems shall not be added to Desktops unless authorized and documented by an authorized person
- All Desktops shall have password protected authorized Screen Savers with timeouts of 10 minutes or less
- The Operating system of all Desktops shall remain up to date with latest Service Packs, Patches and Hot fixes as per Patch Management Policy.
- Anti-virus software shall be installed on all the Desktops and the Anti-virus definitions shall be updated regularly as per Anti-Virus Policy
- Folders and disk drives on the Desktops shall not be shared unless protected with strong access controls

24.2.4 Acceptable Usage:

- Users shall log out before leaving the Desktop unattended
- Storage of sensitive data on the Desktops shall be minimized.
- Keep backup of the critical files and folders as per Backup Policy
- Necessary precaution shall be taken by the Desktop Users to ensure confidentiality and integrity of data stored in the Desktop

24.2.5 Reuse of Desktop

- Desktops shall be reissued only after obtaining a written consent from the Owner
- Reissued desktops shall be reformatted before being issued to another User

24.3 Communication of Policy Details

This policy and relevant specific policies, procedures shall be published on Company's Intranet and communicated to employees and relevant external parties.

24.4 Periodical Review

The information security policy shall be reviewed on yearly basis or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

The Information Security Management Forum would review this Policy, the compliance and implementation status, effectiveness of controls and their implementation, taking into account Internal Audit Reports, Incidents, suggestions and feedback from related parties and make appropriate recommendation for improvements.

24.5 Violation of the Information Security Policy

Non-compliance or violation of the CIPL's Information Security policy shall result in disciplinary action as per the CIPL's Human Resource Policy and other such rules prevalent at the time of violation.

24.6 ISO controls

- A.9.1.1 Access Control
- A.9.3 User responsibilities

24.7 References

- Access Control Policy - Logical
- Network Policy
- Anti-Virus Policy

25. Daily Monitoring Policy – PO – 25

25.1 Purpose

The policy defines the monitoring and logging framework necessary to deter and / or detect improper behaviors, to foster user accountability, and to allow expedient systems management. All user activities affecting production information have to be monitored and logged in a re-constructive manner. These logs are important for error correction, forensic auditing, security breach investigation and related efforts.

25.2 Policy Details

This policy covers all information and associated IT infrastructure and facility management services within CIPL.

25.2.1 Policy

- IT Manager has right to monitor use of information associated with IT infrastructure and facility management services at its discretion, and shall install monitoring systems to deter and / or detect misuse and intrusion on all key systems and network boundaries (ref A.12.4).
- All highly critical network devices such as routers, firewall, switches and critical servers shall be configured to monitor log recording of user activities, exceptions, and information security events shall be recorded, stored and produced when required.(Ref A.12.4.1)
- The activities carried out by server's administrators and contract employees shall be recorded. These records shall be stored and produced when required(refA.12.4.3)
- All monitored highly critical devices such as servers, firewall, IDS, applications; file integrity monitoring system etc. shall have their system clock synchronized with NTP servers for consistent and meaningful logged information.
- Monitoring and logging devices and software shall be protected from unauthorized use and other internal or external attacks that may deactivate the logging process and / or modify to delete the logs themselves(A.12.4.1)
- Logging facility and logs of monitored devices shall be protected from tampering and un-authorised access. The logs should be securely stored to provide evidences during audits.
- In event of a fault and security incident, the logs shall be used for investigation, prosecution and disciplinary action.(PR-14 Human resource Procedure and Human resource Policy)
- Periodical audits and review of all logs generated by monitored devices shall be the responsibility of CISO.
- Current list of access privileges of each user for each information system and IT asset shall be securely retained. Approved Access request Forms of all users shall be securely retained in digital and physical form with System admin and CISO.
- Manager IT retains the right to report any illegal activities to the appropriate authorities and take legal action in case of severe legal and security breach.

25.3 Communication of Policy Details

This policy and relevant specific policies, procedures shall be published on Company's Intranet and communicated to employees and relevant external parties.

25.4 Periodical Review

The Outsourcing policy shall be reviewed on yearly basis or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

The Information Security Management Forum would review this Policy, the compliance and implementation status, effectiveness of controls and their implementation, taking into account Internal Audit Reports, Incidents, suggestions and feedback from related parties and make appropriate recommendation for improvements.

25.5 Violation of the Information Security Policy

Non-compliance or violation of the CIPL's Outsourcing policy shall result in disciplinary action as per the CIPL's Human Resource Policy and other such rules prevalent at the time of violation.

25.6 ISO controls

- A.12.4.1 Audit Logging
- A.12.4.2 Protection of logs information
- A.12.4.3 Administrator and operators logs

25.7 References

- Information Security Policy
- Internal Audit Policy
- Human Resources Procedure

26. BCP DR Policy – PO – 26

26.1 Purpose

This policy addresses the risks to the business pertaining to non-availability of Information / IT resources due to any short or long-term disruptions.

26.2 Policy Details

This policy shall be applicable to all the highly critical, critical information / IT systems owned by the organization at all geographical locations.

26.2.1 Ownership

Roles:

The Business Continuity Team shall be headed by the (Members from Information Security Management Forum); who shall be the Owner of the Business Continuity Plan. The owner shall be vested with the power of declaring a disaster after granting permission from Information Security Management Forum.

Responsibility:

- Identifying the team members for BCP.
- Developing and implementing the BCP.
- Declaring a disaster and activating the BCP team.
- Minimizing the impact of the incident / disaster event and recovering the identified critical assets as per the Business Continuity Plan.
- Training the team members.
- Testing and keeping the BCP up-to-date.

26.2.2 Identification of Business Continuity Team

- The team shall meet within stipulated period to reiterate the roles and responsibilities of each of the members and the minutes shall be documented. The minutes of these meetings shall be maintained for audit and the issues raised in this meeting shall be addressed within before the next meeting.
- Risk Assessment for Business Impact covering all Highly Critical process and Critical IT assets shall be undertaken by Technology Department in co – ordination with Business head to determine the requirements for DRP as per Risk Assessment Procedure covering:
    - Identification of risks. (Ref.A.17.1.1)
    - Identification of business requirements for continuity. (Ref.A.17.1.2)
    - Quantification of impact.
    - Establishing recovery priorities

26.2.3 Implementing Business Continuity Plan (Ref.A.17.1.3):

- The selected team members shall be trained in their roles and responsibilities as defined within the process.
- An awareness campaign shall be conducted for the general users of information systems assets.
- The asset owner shall define the Maximum Acceptable Outage i.e. the maximum time during which the business shall not be affected.
- The asset owner shall define the Recovery Time Objective for the asset to define appropriate recovery architecture for the asset. The asset owner shall ensure that appropriate Recovery Architecture is defined, so that the asset can be recovered within the Recovery Time Objective. The asset owner shall ensure that the recovery architecture and backup requirements are implemented as defined.
- The asset owner and Technology Department shall define the sequence and priority for recovery from the disaster.
- Roles and responsibilities for initiating the DRP shall be assigned to Technology Department.

26.2.4 Developing BCP Plan (Ref.A.17.1.2, A.17.1.2)

- The team shall identify and classify the types of Incidents.
- The team will define the recovery strategy for associated information asset.
- Defining roles and responsibilities of team members during disaster.
- The BC plan shall be reviewed at least yearly by Asset owner & owner.
- BC Plan is an internal document and hence appropriate access controls shall be implemented over the soft and hard copies of the plan.
- DR plan shall be communicated to all members of the relevant Departments. This shall also be circulated to key functional managers and officials to ensure co-ordination and co-operation with Technology Department in event of invoking DRP.
- A formal Backup Procedure, to aid the BCP and DRP, shall be prepared by Technology department and approved by the ISMS Forum. The Backup Procedure shall be based on Risk Assessment and inputs from the information owners to clearly identify the data to be backed up, backup frequency and archival rules for defining backup procedures and guidelines.
- A procedure to ensure that all employees, third party vendors, contractors, and visitors are protected from the risks of fire, appropriate evacuation procedures shall be developed, drafted, implemented and periodically tested.
- The BCP and DRP shall be tested and reviewed periodically for the following reasons, but not limited to: (Re.A.17.1.3)
    - Business Plans
    - Environment changes
    - Infrastructure changes
    - Personnel changes
    - regulatory requirements

26.2.5 Testing of BCP plan (Ref.A.17.1.3)

A proper test plan shall be finalized and implemented as and when required or at least once in a year to ensure its proper functionality and training to the BC team members. The BC Test Plan shall specify

- the type of test,
- the expected period of recovery
- frequency for such tests,

- the test results shall be submitted to the Board of Directors with an evaluation of the BCP
- the results of the BC tests shall be documented and used for fine tuning the BCP

26.2.6 Audit Trails:

The Data-Center In-charge, on behalf of the Owner, shall:

- implement methodologies to generate adequate and secure audit trails of access, as per Audit Trail Policy, to ensure accountability and to monitor access violations (A.12.4.1)

26.2.7 Backup

- Backup of the Operating System will be as per Backup Policy.

26.3 Communication of Policy Details

This policy and relevant specific policies, procedures shall be published on Company's Intranet and communicated to employees and relevant external parties.

26.4 Periodical Review

The information security policy shall be reviewed on yearly basis or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

The Information Security Management Forum would review this Policy, the compliance and implementation status, effectiveness of controls and their implementation, taking into account Internal Audit Reports, Incidents, suggestions and feedback from related parties and make appropriate recommendation for improvements.

26.5 Violation of the Information Security Policy

Non-compliance or violation of the CIPL's Information Security policy shall result in disciplinary action as per the CIPL's Human Resource Policy and other such rules prevalent at the time of violation.

26.6 ISO controls

- A.17.1.2 – including info security in the business continuity management process
- A.17.1.1 – Business Continuity and risk assessment
- A.17.1.2 - Developing and implementing continuity plans including formation security
- A.17.1.2 - Business Continuity planning framework
- A.17.1.3 – Testing, maintaining and re-assessing BCP
- A.12 .4.1 – Fault Logging

26.7 References

- Information Security Policy
- Risk Assessment Procedure

- BCP DR Procedure

27. Procurement of Hardware and Software Policy – PO – 27

27.1 Purpose

This policy addresses the compliance requirements pertaining to the purchasing or licensing terms and conditions that regulate the use of any Hardware / Software acquired or used.

27.2 Policy Details

This policy is applicable to all employees, vendors, temporary employees, consultants and others working in CIPL.

27.2.1 Policy Statement:

- Purchase of hardware and software shall be in accordance with the Change Management Policy.
- All the purchases shall be evaluated for security requirements. (Ref. A.14.1.1)
- All the equipment purchased shall be provided with insurance coverage to distribute the risk. (Ref.A.17.1.2)
- Information Technology Department shall be aware of all licensing requirements before acquiring hardware / software.
- Information Technology Department shall retain software licenses, master disks, manuals etc. as proof of ownership.
- Information Technology Department, with the help of Purchase department, shall enter into Service Level Agreement wherever necessary for Warranty and AMC Period
- Information Technology Department shall standardize the Operating System and Office Automation software with their version numbers and releases for a common office environment, which shall be loaded on all the Organization's desktops. Operation Department shall ensure availability of adequate number of software licenses for this purpose.
- Information Technology shall ensure that unauthorized software shall not be installed on any IT system.
- Business applications software shall be provided to users as per their business requirement specified by a Department / Functional Head. Any deviations from this shall require specific approval as per relevant procedure.
- During the purchases Purchase Department shall be aware of lead time and high costing of equipment and material to be purchase, which shall not become bottle neck in future. (Ref.A.12.1.3)
- No employee shall make or use unauthorized copies of any software or application.
- Trial ware, beta evaluation versions and games shall not be downloaded from the Internet or copied from any other media.

27.3 Communication of Policy Details

This policy and relevant specific policies, procedures shall be published on Company's Intranet and communicated to employees and relevant external parties.

27.4 Periodical Review

The information security policy shall be reviewed on yearly basis or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

The Information Security Management Forum would review this Policy, the compliance and implementation status, effectiveness of controls and their implementation, taking into account Internal Audit Reports, Incidents, suggestions and feedback from related parties and make appropriate recommendation for improvements.

27.5 Violation of the Information Security Policy

Non-compliance or violation of the CIPL's Information Security policy shall result in disciplinary action as per the CIPL's Human Resource Policy and other such rules prevalent at the time of violation.

27.6 ISO controls

- A.12.1.3 Capacity Management
- A.14.1.1 Security Requirements analysis and Specification
- A.17.1.2 Including information security in the business continuity management Process

27.7 References

- Information Security Policy
- Human Resource Policy
- Change Management Policy.
- Procurement of Hardware and Software Procedure

28. Network Time Synchronization Policy – PO – 28

28.1 Purpose

The purpose of this policy is to define the requirement that all systems in the CIPL technology ecosystem deploy a time synchronization service to ensure consistent usage of time for logging.

28.2 Policy Details

28.2.1 Scope

This policy applies to all individuals managing a computing or technology resource owned or operated by CIPL or anyone operating servers hosted by CIPL.

28.2.2 Responsibility for Implementation

Network Team shall have the responsibility and authority to cause this policy to be implemented and maintained.

28.2.3 Policy Statement

- All systems covered by the scope of this policy must deploy clock synchronization technology to ensure consistent and usable timestamps for activity logging where possible.
- At present, this means that all systems should use Network Time Protocol (NTP) to synchronize each server's as well as network Equipments clock with the NTP server at CIPL.
- All Active Directory connected systems may synchronize time from their domain controllers if those domain controllers are synchronized to the campus NTP server.

28.3 Communication of Policy Details

This policy and relevant specific policies, procedures shall be restricted and shall only be communicated to Network Team.

28.4 Periodical Review

The information security policy shall be reviewed on yearly basis or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

The Information Security Management Forum would review this Policy, the compliance and implementation status, effectiveness of controls and their implementation, taking into account Internal Audit Reports, Incidents, suggestions and feedback from related parties and make appropriate recommendation for improvements.

28.5 Violation of the Information Security Policy

Non-compliance or violation of the CIPL's Information Security policy shall result in disciplinary action as per the CIPL's Human Resource Policy and other such rules prevalent at the time of violation.

28.6 ISO controls

- Not Applicable

28.7 References

- Human Resource Policy

29. Vulnerability Management Policy – PO – 29

29.1 Purpose

The purpose of this policy is to define the requirements for notification, testing, and installation of security-related patches on devices connected to CIPL networks.

29.2 Policy Details

29.2.1 Scope

- This policy applies to all individuals managing a computing or technology resource owned or operated by CIPL or anyone operating servers hosted by CIPL.
- This policy applies to all departments of CIPL
- This policy applies to all electronic devices connected to CIPL networks (public and private) including but not limited to computer workstations and servers, network switches and routers, specialized laboratory equipment, etc.

29.2.2 Responsibility for Implementation

Admin/ Network Team shall have the responsibility and authority to cause this policy to be implemented and maintained.

29.2.3 Policy Statement

It is the stated goal of the CIPL to provide secure IT resources and services in order to protect institutional information assets, as well as the privacy of individual students, faculty, staff, patients, and other entities with which the institution has contractual obligations.

In doing so, CIPL must comply with applicable laws, regulations, and other university or unit policies regarding protection of systems and data. The timely and consistent application of vendor-supplied security patches or mitigation of a reported vulnerability are critical components in protecting CIPL, systems, and data from damage or loss due to threats such as worms, viruses, data loss, or other types of external or internal attacks.

CIPL authorized the IT Security Office and Information Security Office to conduct routine scans of devices connected to CIPL networks to identify operating system and application vulnerabilities on those devices.

CIPL require all administrators of systems connected to CIPL networks to routinely review the results of vulnerability scans and evaluate, test and mitigate operating system and application vulnerabilities appropriately, as detailed in the Vulnerability Management Process. Should an administrator identify a reported vulnerability as a potential false positive, the appropriate security office should be engaged to verify.

29.2.4 Responsibilities

System and application administrators are responsible for assessment and application of security patches that impact systems under their management and supervision.

29.2.5 Exceptions

Requests for exceptions to this policy (requests to not scan a device) may be granted for systems with other security measures (e.g., network filtering, firewall, etc.) in place to mitigate risk.

Any requests must be submitted in writing to the appropriate CISO for review and approval. Exception requests must include:

- Why the scanning exception is being requested.
- Risk to the enterprise of not scanning the device.
- Mitigation of controls that have been implemented, and date of implementation.
- End date for the exception (not to exceed 6 months from the request date).
- In the case of systems or applications managed by departmental or school IT staff, endorsement of the request by the relevant IT staff

29.3 Communication of Policy Details

This policy and relevant specific policies, procedures shall be published on Company's Intranet and communicated to employees and relevant external parties.

29.4 Periodical Review

The information security policy shall be reviewed on yearly basis or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

The Information Security Management Forum would review this Policy, the compliance and implementation status, effectiveness of controls and their implementation, taking into account Internal Audit Reports, Incidents, suggestions and feedback from related parties and make appropriate recommendation for improvements.

29.5 Violation of the Information Security Policy

Non-compliance or violation of the CIPL's Information Security policy shall result in disciplinary action as per the CIPL's Human Resource Policy and other such rules prevalent at the time of violation.

29.6 ISO controls

- A.5.1.1 Policies for Information security

- A.5.1.2 Review of the Policies for information security

29.7 References

- Human Resource Policy

30. Management Review Policy – PO – 30

30.1 Purpose

The purpose of the policy is to ensure that organization follows ISMS Monitoring and review policy by conducting Internal ISMS audits and management review of finding to ensure compliance to ISO 27001 security processes for Ensure its continuing suitability, adequacy and effectiveness and to assess opportunities for improvement and the need for change to ISMS, Information Security Policy and Procedures.

30.2 Policy Details

30.2.1 Scope

This policy applies to all CISO, CTO and CEO as well as any individual or Departments managing ISMS implementation.

30.2.2 Responsibility for Implementation

CISO shall have the responsibility and authority to cause this policy to be implemented and maintained.

30.2.3 Policy Statement

CISO shall call for and conduct management review meeting for ISMS once in 6 months or year.
Agenda of Management review can be one of the following

- Results of ISMS audits and reviews
- Feedback from related departments, users, parties
- Techniques, products or procedures, which could be used in organization to improve the ISMS performance and effectiveness
- Status of corrective actions
- Vulnerabilities or threats not adequately addressed in the previous risk assessment
- Follow-up actions from previous management reviews
- Any changes that could affect the ISMS
- Any recommendations for improvement
- Any other suggestions by the members
- Minutes / Output of ISMF meeting

Minutes of MR meetings shall be kept along action planned and taken will be maintained.

30.3 Communication of Policy Details

This policy and relevant specific policies, procedures shall be published on Company's Intranet and communicated to employees and relevant external parties.

30.4 Periodical Review

The information security policy shall be reviewed on yearly basis or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

The Information Security Management Forum would review this Policy, the compliance and implementation status, effectiveness of controls and their implementation, taking into account Internal Audit Reports, Incidents, suggestions and feedback from related parties and make appropriate recommendation for improvements.

30.5 Violation of the Information Security Policy

Non-compliance or violation of the CIPL's Information Security policy shall result in disciplinary action as per the CIPL's Human Resource Policy and other such rules prevalent at the time of violation.

30.6 ISO controls

- NA

30.7 References

- Human Resource Policy

31. Corrective Action Policy – PO – 31

31.1 Purpose

The purpose of this policy is to provide for overall guidelines, and to assign responsibilities for initiating, requesting, implementing, and verifying the effectiveness of corrective and preventative actions. It also establishes methods for taking corrective actions to eliminate the causes of Non-conformance, which would lead to regulatory non-compliance, and prevent their recurrence. Corrective actions must be appropriate to the effects of the nonconformities encountered.

31.2 Policy Details

31.2.1 Scope

This policy applies to preventing and correcting nonconformities related to resources, components, subassemblies, completed services, operational processes, and the quality system.

31.2.2 Responsibility for Implementation

Departments Heads and individuals shall have the responsibility and authority to cause this policy to be implemented and maintained.

Role	Responsibility
Chief Operating Officer (COO)	Approving and allocating company resources to ensure all preventative and corrective actions, when necessary, are carried out throughout CIPL
CEO	Authorization of CAR forms. Review and approval of corrective and preventative actions and implementation timelines. Ensures action implementation and conducts necessary follow-up reviews.
CISO	Completing CAR forms when necessary. Implementing corrective actions and communicating changes to necessary external bodies.

31.2.3 Policy Statement

Corrective action policy that apply to findings from internal and external incident investigations and audits, employee and customer suggestions and management review, to include:

- Method of identifying non-conformities
- Follow-up time frame for initiating corrective action

- Method of tracking initiation and completion of corrective action, including assigned responsibility
- Lessons Learned policy and procedures, to include communication procedures for disseminating lessons learned
- Appropriate corrective action procedures shall be drafted and approved by CISO.

Required Corrective Procedure shall also include following elements

- Written corrective actions for deficiencies identified during external & internal incident investigations and audits
- Method of tracking corrective actions include assigning responsibility
- Method of tracking corrective actions include management review
- Method of tracking include time frame for follow-up for initiating corrective actions Ø Method of tracking include initiation and completion of corrective actions
- Method of identifying non-conformities
- Written procedures for addressing and communicating lessons learned Ø Written corrective actions for deficiencies identified during maintenance
- Written corrective actions for deficiencies identified during employee and customer suggestions
- Written corrective actions for deficiencies identified during management review
- Following issues or points shall also be taken under Corrective action procedure
- Risk Assessments

    - Management of Change process
    - Inspection of Non-Conformities
    - Key Performance Indicators (KPI) Trending
    - Best Practice Discovery
    - Near Miss Incident Investigations

31.3 Communication of Policy Details

This policy and relevant specific policies, procedures shall be published on Company's Intranet and communicated to employees and relevant external parties.

31.4 Periodical Review

The information security policy shall be reviewed on yearly basis or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

The Information Security Management Forum would review this Policy, the compliance and implementation status, effectiveness of controls and their implementation, taking into account Internal Audit Reports, Incidents, suggestions and feedback from related parties and make appropriate recommendation for improvements.

31.5 Violation of the Information Security Policy

Non-compliance or violation of the CIPL's Information Security policy shall result in disciplinary action as per the CIPL's Human Resource Policy and other such rules prevalent at the time of violation.

31.6 ISO controls

- NA

31.7 References

- Human Resource Policy

32. Capacity Management Policy – PO – 32

32.1 Purpose

This policy establishes the organizational policy for planning and performing the Capacity Management process to ensure that all current and future capacity and performance aspects of the Information Technology (IT) infrastructure within CIPL offices at Mumbai and DR site are provided to meet business requirements at acceptable cost. The Capacity Management process ensures IT infrastructure is provided at the right time in the right volume at the right price, and ensures that IT is used in the most efficient manner.

32.2 Policy Details

32.2.1 Scope

This policy applies to all individuals or Departments managing a computing or technology resource owned or operated by CIPL.

32.2.2 Responsibility for Implementation

Departments Heads and individuals shall have the responsibility and authority to cause this policy to be implemented and maintained.

Department Head shall ensure that the following key activities are performed in accordance with the defined Capacity Management Process:

- Demand management for business, service, and component capacity activities
- Analyzing Capacity Requirement for business, service, and component capacity activities
- Application sizing for business, service, and component capacity activities
- Capacity planning for business, service, and component capacity activities
- Capacity monitoring and analysis
- Implementation of capacity-related changes
- Control of storage capacity monitoring data for capacity activities
- Provide to management information about Capacity Management performance and operations

32.2.3 Policy Statement

All department heads such as

- Operations (Network, Data center, System Administration)
- Information Technology
- Human Resources
- Administration
- CISO

Shall use capacity Management process to define

- Business Capacity - The process shall be used to forecast capacity needs based on business events.
- Service Capacity - The process shall be used to ensure capacity levels support established service level targets.
- Component Capacity - The process shall be used to ensure capacity levels are provided for the individual IT device level.

Each Department shall use capacity management process by taking following steps

- Determine capacity requirements
- Analyze current capacity
- Plan for the future capacity
- Finalize capacity requirements
- Approve capacity requirements

Departments	Capacity Requirement for
Operations	Manpower Support, Administration
Information Technology	Hardware Numbers
	Hardware servers capacity/sizing for applications
	Hardware servers capacity/sizing for database
	Hard-disk capacity for Database objects
	Hardware sizing /numbers for network
	Network topology for performance
	Data center capacity
Human Resources	Manpower Requirements
	Hardware Requirements
Administration	Supporting devices like AC, UPS, Access Control etc.
Chief Information Security Officer – CISO	Resources to Manage Information Security

Capacity planning shall be documented and approved.

32.3 Communication of Policy Details

This policy and relevant specific policies, procedures shall be published on Company's Intranet and communicated to employees and relevant external parties.

32.4 Periodical Review

The information security policy shall be reviewed on yearly basis or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

The Information Security Management Forum would review this Policy, the compliance and implementation status, effectiveness of controls and their implementation, taking into account Internal Audit Reports, Incidents, suggestions and feedback from related parties and make appropriate recommendation for improvements.

32.5 Violation of the Information Security Policy

Non-compliance or violation of the CIPL's Information Security policy shall result in disciplinary action as per the CIPL's Human Resource Policy and other such rules prevalent at the time of violation.

32.6 ISO controls

- A. 12.1.3 Capacity Management

32.7 References

- Human Resource Policy

33. Clear Desk and Clear Screen Policy – PO – 33

33.1 Purpose

The purpose of this policy is to improve the security and confidentiality of information, the CIPL has adopted a clear desk policy for papers and removable storage media, and clear screen policy for information processing facilities. This is to reduce the risk of unauthorized access, loss of, and damage to information during and outside normal working hours or when areas are unattended.

33.2 Policy Details

This policy applies to all individuals managing a computing or technology resource owned or operated by CIPL or anyone operating servers hosted by CIPL.

Review/Monitoring Arrangements All employees are responsible for monitoring their compliance with the principles / procedures detailed in this policy; departmental managers and project managers should also monitor compliance on a regular basis.

Departments Heads and individuals shall have the responsibility and authority to cause this policy to be implemented and maintained.

33.2.1 Clear Desk

Where practically possible, paper and computer media should be stored in suitable locked safes, cabinets or other forms of security furniture when not in use, especially outside working hours. • Where lockable safes, filing cabinets, drawers, cupboards etc. are not available, office / room doors must be locked if left unattended. At the end of each session all sensitive information should be removed from the work place and stored in a locked area.

This includes all patient identifiable information, as well as business critical information such as salaries and contracts.

- Confidential sensitive or classified information, when printed, should be cleared from

printers immediately. Where possible printers with a 'locked job' facility should be used.

- It is good practice to lock all office areas when they are not in use.
- Any visit, appointment or message books should be stored in a locked area when not in use.
- The reception desk can be particularly vulnerable to visitors. This area should be kept as clear as possible at all times; in particular medical records or other person identifiable information should not be held on the desk within reach/sight of visitors.
- It is also worth noting that information left on desks is also more likely to be damaged or destroyed in a disaster such as fire, flood or explosion.

33.2.2 Clear Screen

- CIPL computers / computer terminals should not be left logged on when unattended and should be password protected.
- Computer screens should be angled away from the view of unauthorized persons.
- The Windows Security Lock should be set to activate when there is no activity for a short pre-determined period of time.
- The Windows Security Lock should be password protected for reactivation.
- Users should log off or lock their machines (by pressing the Windows key and L) when they leave office

33.3 Communication of Policy Details

This policy and relevant specific policies, procedures shall be published on Company's Intranet and communicated to employees and relevant external parties.

33.4 Periodical Review

The information security policy shall be reviewed on yearly basis or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

The Information Security Management Forum would review this Policy, the compliance and implementation status, effectiveness of controls and their implementation, taking into account Internal Audit Reports, Incidents, suggestions and feedback from related parties and make appropriate recommendation for improvements.

33.5 Violation of the Information Security Policy

Non-compliance or violation of the CIPL's Information Security policy shall result in disciplinary action as per the CIPL's Human Resource Policy and other such rules prevalent at the time of violation.

33.6 ISO controls

- A. 11.2.9 Clear Desktop and Clear screen Policy

33.7 References

- Human Resource Policy

34. Monitoring & Measurement Policy – PO – 34

34.1 Purpose

The purpose of this policy is to define information security objectives / metrics for monitoring and measurement of activities. This is to collect the data from respective departments based on the frequency defined. This helps in controlling activities related to respective departments for better improvements.

34.2 Policy Details

34.2.1 Scope

This policy applies to all individuals departments where security objectives are defined and where data needs to be collected and monitored CIPL.

34.2.2 Responsibility for Implementation

Departments Heads and individuals shall have the responsibility and authority to cause this policy to be implemented and maintained.

34.2.3 Policy Statement

- HODs shall identify security controls those are most critical to their operations and establish metrics for these.
- HODs shall monitor the information assets based on predefined metrics and records collected for defined period
- HODs shall analyze these details to identify and highlight the root-cause of metric performance or lack thereof.
- HODs shall analyze Incident Register reporting Information Security incidents and weaknesses and the data used for evaluating the effectiveness.
- HODs shall report all information security incidents, weaknesses/vulnerabilities, non-conformities and metric performance data periodically to the Management.
- HODs analyze root-cause analysis for reported incidents maintained in the incident register.
- HODs make an attempt to correlate reported incidents and weaknesses back to the ineffectiveness of implemented controls.
- HODs shall analyze Audit findings, if any, during the defined period and considers as indicators of the effectiveness of security controls.
- HODs shall identify all metrics in Metric Report to measure the effectiveness of controls have been defined as a percentage to enable a holistic picture of the status of the control and its performance.
- The first three months of effectiveness measurement data shall be analysed and studied to arrive at a baseline (either average or minimum) and subsequent metric data for that control shall be compared against the baseline value to justify further investigation into metric performance.

34.3 Communication of Policy Details

This policy and relevant specific policies, procedures shall be published on Company's Intranet and communicated to employees and relevant external parties.

34.4 Periodical Review

The information security policy shall be reviewed on yearly basis or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

The Information Security Management Forum would review this Policy, the compliance and implementation status, effectiveness of controls and their implementation, taking into account Internal Audit Reports, Incidents, suggestions and feedback from related parties and make appropriate recommendation for improvements.

34.5 Violation of the Information Security Policy

Non-compliance or violation of the CIPL's Information Security policy shall result in disciplinary action as per the CIPL's Human Resource Policy and other such rules prevalent at the time of violation.

34.6 ISO controls

- 9.1 Monitoring, measurement, analysis and evaluation

34.7 References

- Human Resource Policy

35. Cryptography Policy – PO – 35

35.1 Purpose

The purpose of this cryptographic policy is to define the acceptable use and management of cryptographic software, API, cryptographic routines, classes and hardware throughout CIPL.

35.2 Policy Details

35.2.1 Scope

This policy applies to

- The policy applies to: All Information Technology (I.T.) resources provided by the CIPL
- All users (including CIPL staff, contractors, sub-contractors, agency staff and authorized third party commercial service providers) of the CIPL's I.T resources
- All connections to (locally or remotely) the CIPL network Domains (LAN/WAN/Wi-Fi)
- All connections made to external networks through the CIPL network.

35.2.2 Responsibility for Implementation

Departments Heads and individuals shall have the responsibility and authority to cause this policy to be implemented and maintained.

35.2.3 Principles of cryptography

Where possible all confidential and restricted information must be stored on a secure CIPL network server with restricted access. Where it has been deemed necessary by a CIPL IT manger to store confidential or restricted information on any device other than a CIPL network server the information must be encrypted.

All confidential and restricted information transmitted via email to an email address outside of the CIPL domain (i.e. one that does not end in "i.e. @CIPL.com.") must be encrypted and sensitive information must be masked.

All passwords used as part of the process to encrypt/decrypt information must meet the requirements of the CIPL Password Policy

35.2.4 Servers

Confidential and restricted information stored on shared CIPL network servers which are situated in physically insecure locations (For example remote file/print servers) must be protected by the use of strict access controls and encryption software.

All backup data where sensitive information is present must be encrypted.

35.2.5 Desktop Computers

CIPL desktop computers are generally accepted as having a lower risk of being stolen and as such most will not need to have encryption software installed. However the following types of CIPL desktop computers will need to have encryption software installed.

35.2.6 Laptop, Mobile Computer & Smart Devices

All CIPL laptop computer devices must have CIPL approved encryption software installed prior to their use within the CIPL. In addition to encryption software the laptop must be password protected and have up to date anti-virus software installed.

CIPL mobile computer devices & smart devices must have device encryption enabled or CIPL approved encryption software installed prior to their use within the CIPL.

The preferred method of encryption for laptop computers, mobile computer devices and smart devices is whole disk encryption. Mobile computer devices and smart devices which are not capable of whole disk encryption must use file/folder level encryption to encrypt all confidential and restricted information stored on the device.

Laptop, mobile computer devices and smart devices must not be used for the long-term storage of confidential and restricted information.

35.2.7 Removable Storage Devices

All confidential and restricted information stored on removable storage devices must be encrypted. In addition to being encrypted, removable storage devices must be stored in a locked cabinet or drawer when not in use.

Removable storage devices except those used for backup purposes must not be used for the long-term storage of confidential and restricted information.

The preferred method of encryption for removable storage devices is whole disk/device encryption. Where whole disk encryption is not possible, then file/folder level encryption must be used to encrypt all confidential and restricted information stored on the removal storage device.

35.2.8 USB Memory Sticks

Confidential and restricted information may only be stored on CIPL approved encrypted USB memory sticks which are available from the security. The storage of confidential or restricted information on any other USB Drive/USB memory sticks (encrypted or otherwise) will be considered a breach of this policy.

CIPL approved USB memory sticks must only be used on an exceptional basis where it is essential to store or temporarily transfer confidential or restricted information. They must not be used for the long term storage of confidential or restricted information, which must where possible be stored on a secure CIPL network server.

Confidential and restricted information stored on the CIPL approved USB memory stick must not be transferred to any internal (except a secure CIPL network server) or external system in an unencrypted form.

35.2.9 Transmission Security

All confidential or restricted information transmitted through email to an email address outside of the CIPL domain (i.e. one that does not end in "@saraswtbank.com.ie") must be encrypted. The transfer of such information outside of the CIPL domain must be authorized by a CIPL IT manager. The authorization must be issued in advance of the first instance and will apply thereafter if necessary.

Where confidential and restricted information is transmitted through a public network (for example the internet) to an external third party the information must be encrypted first or sent via a secure channels (for example: Secure FTP, TLS, VPN etc.). The transfer must be authorized by a CIPL IT manager. The authorization must be issued in advance of the first instance and will apply thereafter if necessary.

35.2.10 Approved Encryption Algorithms and Protocols

- **Symmetric Key Encryption Algorithms**
  - Triple Data Encryption Standard (3DES) - (Minimum encryption key length of 168 bits)
  - Advanced Encryption Standard (AES) - (Minimum encryption key length of 256 bits)
  - Blowfish - (Minimum encryption key length of 256 bits)
- **Asymmetric Key Encryption Algorithms**
  - Digital Signature Standard (DSS)
  - Rivest, Shamir & Adelman (RSA)
  - Elliptic Curve Digital Signature Algorithm (ECDSA)
- **Encryption Protocols**
  - IPSec (IP Security)
  - SSL (Secure Socket Layer)

35.2.11 Encryption Key Management

- Key management must be fully/partially automated
- Private keys must be kept confidential in Tamper evident envelopes
- Keys in transit and storage must be encrypted

35.3 Communication of Policy Details

This policy and relevant specific policies, procedures shall be published on Company's Intranet and communicated to employees and relevant external parties.

35.4 Periodical Review

The information security policy shall be reviewed on yearly basis or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

The Information Security Management Forum would review this Policy, the compliance and implementation status, effectiveness of controls and their implementation, taking into account Internal Audit Reports, Incidents, suggestions and feedback from related parties and make appropriate recommendation for improvements.

35.5 Violation of the Information Security Policy

Non-compliance or violation of the CIPL's Information Security policy shall result in disciplinary action as per the CIPL's Human Resource Policy and other such rules prevalent at the time of violation.

35.6 ISO controls

- 10.1.1 Use of Cryptographic Controls
- 10.1.2 Key Management
- 18.1.5 Regulation of Cryptographic Controls

35.7 References

- Human Resource Policy

….END OF POLICY MANUAL….