Information Security Management System Manual

For ISO 27001:2013

Table of Contents

Change History: 6

0. Introduction 8

0.1 Introduction: Clover Infotech Private Limited (CIPL) 8

1. Scope 9

1.1 Scope Statement 9

1.2 Locations and exclusions from the scope 10

2. Normative Reference 12

3. Terms and Definitions 13

3.1 Terms 13

3.2 Definitions ..... 15~~14~~

4. Context of Organization ..... 17~~15~~

4.1 Understanding Organization and its context ..... 17~~15~~

4.1.1 External Context of Organization ..... 17~~15~~

4.1.1.1 Key drivers having impact on the objectives of CIPL ..... 17~~15~~

4.1.1.2 External Issues ..... 17~~15~~

4.1.2 Internal Context of Organization ..... 18~~16~~

4.1.2.1 Information Security Management Forum – ISMF ..... 18~~16~~

4.1.2.2 Internal Issues ..... 19~~17~~

4.2 Understanding the needs and expectations of interested parties ..... 20~~18~~

4.2.1 Interested parties impacting the information security of CIPLare ..... 20~~18~~

4.2.2 Interface and Dependencies ..... 23~~20~~

4.3 Determining the scope of the information security management system ..... 23~~20~~

4.4 Information Security Management System ..... 24~~21~~

4.4.1 Standards, Guidelines, Models used adopted by CIPL ..... 24~~21~~

4.4.2 Framework for building ISMS ..... 24~~21~~

Formatted: Font: 10 pt

4.4.3 List of Processes incorporated in the Information Security Management System 2522
5. Leadership 2623
5.1 Leadership and Commitment 2623
5.1.1 General / Management Responsibilities 2623
5.1.2 Customer Focus 2623
5.1.3 Organization Chart 2724
5.2 CIPL's Information Security Policy Statement 2825
5.2.1 Communicating the Security Policy 2825
5.3 Organizational Roles, Responsibilities and Authorities 2926
5.4 CISO 2926
6. Planning 3027
6.1 Actions to address risks and opportunities 3027
6.1.1 Statement of applicability 3027
6.2 Information Security Objectives and planning to achieve them 3027
6.2.1 Information Security Objectives 3027
6.2.2 Security Awareness Program 3128
6.2.3 Security Metrics and Measurement 3228
6.2.4 Legal or Regulatory Requirements 3229
6.2.5 Review 3330
7. Support 3330
7.1 Resources 3330
7.2 Competence 3330
7.3 Awareness 3330
7.4 Communication 3532
7.5 Documented Information 3633

Formatted: Font: 10 pt

7.5.1 General 3633
7.5.2 Creating and Updating 3734
7.5.3 Control of Documented Information 3835
8. Operations 4036
8.1 Operations Planning and Control 4036
8.1.1 Preliminary Review and planning 4036
8.1.2 Identification of Scope of ISMS 4036
8.1.3 Gap Analysis 4036
8.1.4 Risk Assessment 4037
8.1.5 Risk Mitigation and Selection of Controls 4037
8.1.6 Redesign of Security Architecture 4037
8.1.7 Policies and Procedures Drafting 4037
8.1.8 Incident Management 4037
8.1.9 Design of BCP / DRP 4037
8.1.10 Design of Audit Charter 4137
8.1.11 Security Awareness Program 4137
8.1.12 Security Metrics 4137
8.1.13 Implementation of Controls 4138
8.1.14 Internal Audits 4138
8.1.15 Management Reviews 4138
8.2 Information Security Risk Assessment 4138
8.3 Information Security Risk Treatment 4238
8.3.1 Risk Management Decision 4238
9. Performance Evaluation 4340
9.1 Monitoring, Measurement, Analysis and Evaluation 4340

Formatted: Font: 10 pt

9.1.1 Monitoring and Measurement 4340
9.1.2 Customer satisfaction 4340
9.1.3 Monitoring and measurement of processes 4340
9.1.4 Monitoring and measurement 4340
9.1.5 Analysis and Evaluation 4542
9.2 Internal Audit 4542
9.3 Management Review 4743
9.3.1 General 4743
9.3.2 Review Input 4744
9.3.3 Review Output 4744
10. Improvement 4845
10.1 Non-Conformity and Corrective Actions 4845
10.1.1 Non-Conformity 4845
10.1.2 Corrective action 4845
10.2 Continual Improvement 4845

Formatted: Font: 10 pt

Change History:

Sr. No.	Version	Details of Amendment	Author	Date	Approver	Date
1	1.0	Initial Document	CISO	3rd September 2018	MD	3rd September 2018
2	1.1	Addition to the scope of ISMS	CISO	9th January 2019	MD	9th January 2019
3	2.0	Annual Review and MIDC location Added	CISO	13th Nov 2019	MD	16th December 2019
4	3.0	Annual Review and MIDC location removed Font changed to Calibri	CISO	2nd Nov 2020	MD	10th Nov 2020

Formatted: Font: 10 pt

INFORMATION SECURITY MANUAL – LEVEL 01

MANDATORY CLAUSES

Formatted: Font: 10 pt

0. Introduction

0.1 Introduction: Clover Infotech Private Limited (CIPL)

Founded in 1994, Clover Infotech is a comprehensive IT services provider with a strong presence in India, Dubai and the United States of America. Over the years, Clover Infotech has established its expertise across multiple technologies including Oracle, Microsoft and Open Source.

Equipped with ISO 27001 delivery centres, Clover Infotech has been providing services ranging from Application services to Infrastructure management services to over 150 customers across geographies and industry verticals. Clover Infotech is one of Oracle's focused partners for platform and infrastructure cloud services, as well as ERP cloud. The company has also been working on AI-powered intelligent bots to meet the requirements of businesses from across industries.

History

Incorporated in 1994 under the dynamic entrepreneurship ofJaved F. Tapia, Clover Infotech made a head start in providing high quality technology solutions and services to leading organizations in India.

In the year 2000, Clover Infotech entered into a Joint Venture agreement with Red Hat, Inc., USA, to launch Red Hat's operations in the Indian market. Under Mr. Tapia's strategic leadership, Red Hat India Pvt. Ltd. fuelled an Open Source revolution in the country and over the last decade, we have expanded our portfolio to include multiple areas of services including Database Management, Middleware Services, Application Development and Maintenance, ready to deploy Business Solutions and Customised Application Development.

Our Approach

We believe in delivering tangible results for our customers in a cost-effective manner. We do this through a consultative, solution-based approach wherein we gather in-depth understanding of the customer's requirements and facilitate customized solutions.In the process, we ensure greater efficiency and predictability in businesses through a dependable IT infrastructure. We have also introduced dedicated practices Enterprise business solutions & Web, Big Data & Analytics, and Infrastructure services – to deliver innovative solutions for new age businesses.

Formatted: Font: 10 pt

1. Scope

Scope Statement

CIPL "**Management of information security in providing Information Technology services to customers and associated internal support services as per statement of applicability Ver 2.4 dated 09.01.19**". Following are the various departments included under the scope of the ISMS:

System Processes:

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

Operations Processes

- Marketing
- Practices
- Human Resources
- Talent Acquisition
- Project Management Office
- Academy
- Administration
- Information Technology
- Infrastructure Project Delivery
- Resourcing
- Managed IT
- Application Development
- Application Support
- Sales
- Project Management
- Center of Excellence – CoE Process
- Corporate Quality
- Legal and Compliance

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

- Mumbai JBNagar
- Mumbai MIDC
- Pune

Formatted: Font: 10 pt

This policy has been approved by the company management and shall be reviewed by the management review team annually:

Location Activities:

Pune Office: Clover Centrum, Galaxy Society Plot No 5, Boat Club Road, Pune 411 001, India Tele: +91 20 2616 0022 /23 /24 Fax: +91 20 5601 4881	**Mumbai Office**: 2nd Floor, Dhana Singh Processors Building, Vazir Glass Lane, J B Nagar, Andheri (East), Mumbai- 400 059, Maharashtra, India Tele: +91 22 29261650
~~Mumbai MIDC Office:~~ ~~Clover Infotech pvt ltd, 3rd Floor,~~ ~~61 Radius Building, Near Tunga Hotel, MIDC, Andheri East 400093, Maharashtra, India.~~ ~~Tele: +91 22 68524900~~	

Formatted: Highlight

1.1 Locations and exclusions from the scope

CIPLhas its operations running across the following locations:

Sr. No.	Location	Areas of Operations	Scope/Out of Scope
1	Clover Centrum, Galaxy Society Plot No 5, Boat Club Road, Pune 411 001, India Tele: +91 20 2616 0022 /23 /24 Fax: +91 20 5601 4881	• Marketing • Practices • Human Resources • Talent Acquisition • Project Management Office • Academy • Administration • Information Technology • Infrastructure Project Delivery • Resourcing • Managed IT • Application Development • Application Support • Sales • Project Management • Center of Excellence – COE • Corporate Quality	In Scope
2	2nd Floor, Dhana Singh Processors Building,	• Marketing	In Scope

Formatted: Font: 10 pt

Sr. No.	Location	Areas of Operations	Scope/Out of Scope
	Vazir Glass Lane, J B Nagar, Andheri (East), Mumbai- 400 059, Maharashtra, India Tele: +91 22 29261650	• Practices • Human Resources • Talent Acquisition • Project Management Office • Academy • Administration • Information Technology • Infrastructure Project Delivery • Resourcing • Managed IT • Application Development • Application Support • Sales • Project Management • Center of Excellence – COE • Corporate Quality • Legal and Compliance	
~~3~~	~~Clover Infotech pvt ltd, 3rd Floor, 61 Radius Building, Near Tunga Hotel, MIDC, Andheri East 400093, Maharashtra, India. Tele: +91 22 68524900~~	• ~~Academy~~ • ~~Administration~~ • ~~Information Technology~~ •	~~In Scope~~

Formatted: Highlight

Formatted: Font: 10 pt

2. Normative Reference

The following normative document contains provisions, which through reference in this text constitute provisions of this International Standard.

ISO 27001:2013. Information Security Management Systems – Fundamentals and vocabulary are purchased and same documents are controlled as external originated documents.

Any other document related to Customers will be identified, listed as an external originated documents and appropriate controls also will be made.

ISO 9001:2015 Quality Management Systems – Fundamentals and vocabulary are purchased and same documents are controlled as external originated documents.

References:

External originated document: ISO 27001:2013 Standard
External originated document: ISO 9001:2015 Standard & Documents / Records

Formatted: Font: 10 pt

3. Terms and Definitions

Purpose of this International Standard, the terms and definitions given in ISO 27001 apply.

ISO 27001:2013. Information Security Management Systems – Fundamentals and vocabulary are purchased and same documents are controlled as external originated documents.

ISO 9001:2015 Quality Management Systems – Fundamentals and vocabulary are purchased and same documents are controlled as external originated documents.

References:

External originated documents: ISO 27001:2013 Standard
External originated document: ISO 9001:2015 Standard & Documents / Records

3.1 Terms

Abbreviation	Description
CIPL	Clover Infotech Pvt. Ltd.
ISO	International Organization for Standardization
CISO	Chief Information Security officer
ISMS	Information Security Management System
SOP	Standard Operating Procedure
MD	Managing Director
HOD	Head of Department
MKT	Marketing
TRG	Training
IQA	Internal Quality Audit
VP	Vice President
PO	Purchase Order
WO	Work Order
CA	Corrective Action
NC	Non-Conformity
CI	Continual Improvement
Sr. No.	Serial Number
PM	Project Manager
PL	Project Leader
TECH	Technical
ADM/ ADMIN	Administration
SYS ADMIN	System Administrator
PUR	Purchase
PRJ	Project
RFP	Request for proposal
BD	Business Development
IT	Information Technology
BRD	Business Requirement Document
HR	Human Resource

Formatted: Font: 10 pt

Abbreviation	Description
COE	Centre of Excellence

Formatted: Font: 10 pt

3.2 Definitions

Definition	Description
Asset	Anything that has a value to CIPL
Confidentiality	Ensuring that information is not available or disclosed to unauthorized individuals, entities or processes
Integrity	Ensuring that information is accurate and complete
Availability	Ensuring that information is being accessible and usable upon demand by an authorized user
Information Security	Preserving the Confidentiality, Integrity and Availability of information along with Authentication, Authorization, Accounting and Non-Repudiation
Information Security Event	An identified occurrence of a system, service, or a network state indicating a possible breach of information security policy or failure to maintain or a previously unknown situation that may be security related
Information Security Incident	Unwanted or unpredicted information security events that have a significant probability of compromising CIPL business operations, associated information processing facilities and information contained within
Information Security System	Overall management system based on business risk and impact analysis, to establish, implement, operate, monitor, review, maintain and improve the information security of assets
Risk	Function of likelihood of occurrence of an event and the associated impact on information processing facilities or information
Threat	A potential cause of an unwanted event or an incident resulting in damage or impairment to a system or organisation as a whole
Vulnerability	A weakness or a flaw in an asset or a group of assets which may be exploited by an attacker / unauthorized user to violate the Confidentiality, Integrity or Availability of the information or the asset
Residual Risk	Risk remaining after risk treatment
Acceptable Risk	Quantity / Level of risk acceptable to the organisation post risk assessment
Risk Assessment	Overall process of identification, analysis, evaluation of vulnerabilities, impact and probability of occurrence of threat affecting information and information processing facilities of organisation
Risk Mitigation	Process of reducing the identified risks to the identified acceptable level
Risk Treatment	Process of managing the identified risks by avoiding (eliminating), reducing (mitigating), transferring (outsourcing), or accepting and budgeting (risk retention)
Risk Management	Risk management is activity directed towards the assessing, mitigating (to an acceptable level) and monitoring of risks
Statement of Applicability	Document describing the control objectives and controls that are relevant and applicable to organisation's ISMS
Information Processing Facilities	Setup established for the provision of sharing, transmitting, storing, processing, assessing, evaluating the information by an organisation through the usage of IT and Non IT related assets
Email / Internet Facility	Provision of electronic mail and Internet access provided by the organisation through its information processing facilities
Access Control	Refers to the processes, rules and deployment mechanisms which control access to information systems, resources and physical access to premises

Formatted: Font: 10 pt

Definition	Description
Authentication	The act of verifying the identity of a user. Verification of the correctness of a piece of data. The eligibility of the user to access certain information resource
Authorization	The granting or refusing of privileges to an entity for accessing specific services

Formatted: Font: 10 pt

4. Context of Organization

4.1 Understanding Organization and its context

4.1.1 External Context of Organization

4.1.1.1 Key drivers having impact on the objectives of CIPL

- Organizational policies of CIPL are governed and approved by the top management of CIPL and the CIPL group. These policies are also governed by the local legal and statutory regulations as listed in the information security policy.
- Changes in management structure will also have an impact on corporate governance and policies as and when these structural changes happen.
- Customer requirements for information security.
- Business need to protect customer's and organization's intellectual property and confidential information
- All information related to vendors/suppliers should be adequately secured.
- Adequate SLA / NDA's are signed between the two interested parties to protect the Information / Confidentiality of the organization.

4.1.1.2 External Issues

Following are the external issues identified for Clover:

1. **Legal and regulatory.**

Clover Infotech recognizes that there are legal and regulatory requirements over and above the requirements as established by our internal requirements.

LEGISLATION	IS REQUIREMENTS
1. Contract law	A contract is a legally enforceable exchange of promises. Any agreement we enter into must follow a set format or it could be invalid
2. Information Technology Act 2000 and its Amendment, 2008	Legislation Covering IT Act 2000 and it amendment 2008, We must ensure that all the requirements of this acts are covered.

2. **Cultural**
   - Personal data (Significant inducements can be offered to staff for the collection of information this could affect "confidentiality".)
   - Hacking and unauthorized interception of communications will affect "confidentiality".
   - Salarydetails (bribery is an ever present threat; this could affect "confidentiality").

Formatted: Font: 10 pt

3. **Connectivity**
   - Power and connectivity
   - International clients are expecting state of the art technology, uninterrupted connection along with necessary speeds for operations. This has an impact on commitments contained in our service level agreements.

4. **Location**
   - Physical location- (location in a commercial area and adjacent offices and so threat of robbery which could have an impact on "confidentiality").
   - Environmental (no particular flooding or storm damage is anticipated).

5. **Competition**
   - Staff can often move from our company to a competitor quickly or share information with the competitor. This could affect "confidentiality".

6. **Economic pressures**
   - This could entail poaching key members of staff and securing access to confidential information. The loss of a key member of staff with the customer data they have access to could impact us heavily. This could affect "confidentiality".
   - In tight financial times customers are seeking cost saving alternatives; we are therefore seeing a large increase in sales enquiries putting pressure on our internal resources and IT and IS systems.

7. **Technological:**

   These factors include technological aspects like research and development, automation, technology incentives, and the rate of technological change. These can determine barriers to entry and minimum efficient production level, as well as, influence outsourcing decisions. Technological shifts affect costs, security, quality, and innovation.

8. **Geographical:**

   These factors include ecological and environmental aspects such as weather, climate, and climate change, which may especially affect the organization

4.1.2 Internal Context of Organization

4.1.2.1 Information Security Management Forum – ISMF

- ISMF is the apex body for guiding the establishment of a structured Information Security Management System at CIPL. The actual implementation would be carried out by the resources from different departments to meet a common goal of management.
- The ISMF governs the establishment, implementation, operation, review, maintenance, and improvement of the information security management system at CIPL.
- Organisational structure and the responsibilities of the ISMF are discussed in the succeeding sections.
- To ensure that mission critical business services are protected and ISMS environment is maintained at all the times in CIPL, the ISMF shall, from time to time, review the information security policies

Formatted: Font: 10 pt

and procedures, audit the security controls implemented, identify the risks pertaining to critical information and associated assets and implement risk treatment controls to mitigate the level of risk which is beyond the acceptable limit of the organisation.

Sr. No.	Name of employee	Designation	Base location	Contact no.	Email
1	Javed Tapia	MD	Mumbai	022-29261650	javed.tapia@cloverinfotech.com
2	Shrikant Navelkar	Director	Pune	020-26160022	shrikant.navelkar@cloverinfotech.com
3	Kunal Nagarkatti	COO	Mumbai	022-29261650	kunal.nagarkatti@cloverinfotech.com
4	Elizabeth Paul	Sr. VP-HR	Mumbai	022-29261650	elizabeth.paul@cloverinfotech.com
5	Suresh Dubey	Head Accounts and Finance	Mumbai	022-29261650	suresh.dubey@cloverinfotech.com
6	Vikram Gite	AVP - Delivery, MR	Mumbai	022-29261650	vikram.gite@cloverinfotech.com
7	Siddharth Deshmukh	Head-Global Delivery	Mumbai	022-29261650	siddharth.deshmukh@cloverinfotech.com
8	Nilesh Bhate	Head-Admin	Mumbai	022-29261650	nilesh.bhate@cloverinfotech.com
9	Prashant Parab	Head - Operations	Mumbai	022-29261650	prashant.parab@cloverinfotech.com
10	Neelesh Kriplani	Head - COE	Pune	022-29261650	neelesh.kripalani@cloverinfotech.com
11	Nisha Bandodkar	Head - QA, Deputy MR	Mumbai	022-29261650	nisha.bandodkar@cloverinfotech.com
12	Preethi Menon	Head – Practices	Mumbai	022-29261650	Preethi.menon@cloverinfotech.com

4.1.2.2 Internal Issues

Following are the internal issues identified for Clover

1. **Information systems**
   - If systems are old and need to be replaced, then new systems may be more complex and possibly harder to support. A possible "integrity" issues.

2. **Organization's culture**
   - A breach between strategic direction and IS policy which could lead to leakage of information.

3. **Relationships and perceptions and values of internal stakeholders**
   - A high turnover in staff may result in data loss. Also, comprehending the nature of IS policies and their importance and consequences may not be fully recognized and hence information security incidents are more likely.
   - If there is a high turnover in staff then chances are there that staff could take data such as documented processes with them on departure which are important

Formatted: Font: 10 pt

- Many skills and decision making authorities are restricted to a very few senior staff who know each other very well, this has led to a competence and documentation „gap" through informality.

4. **Human Resource Security and Capabilities (knowledge)**
   - The high staff turnover causes difficulties in retaining core knowledge, such as system support and customer relations.

5. **Governance, organization and roles and responsibilities**
   - As a small company, responsibilities have been retained by a small management team. As we grow this may be difficult to achieve but is needed.

6. **Standard working procedures and guides**
   - Processes have not been documented as we grow this lack of documentation may cause problems.

7. **Contractual relationships with our suppliers**
   - If IS requirements are not formally mentioned in contracts with any suppliers this will impact "Confidentiality" and "Integrity".

4.2 Understanding the needs and expectations of interested parties

4.2.1 Interested parties impacting the information security of CIPLare

Sr. No.	Interested Party	Type	Information Security Expectations / Requirements
1	Customers	External / Internal	• Unless there are major changes to the overall organization business would not get impacted and likely to grow as per the current trends and as per the historical growth rate achieved. • All information related to clients should be adequately secured. • ISO 27001 compliance • Meeting SLA targets of 99.9% for system availability • Customers are internal from India and Global regions
2	Shareholders	Internal	• Currently 100 % owned by CIPL and only impact resides if there is a change in part or full ownership. • All information related to shareholders should be adequately secured. • Return on capital
3	Employees / Contract Agencies	Internal	• The recruitment and training process is such that the best pool of resources are hired and nurtured. • Attrition is minimal and contingencies are in place so that the business as usual can be managed • Profitable and secure work. • Safe and appropriate work environment.

Formatted: Font: 10 pt

Sr. No.	Interested Party	Type	Information Security Expectations / Requirements
			• Training and support.
4	Vendors / Suppliers / Service Providers	External	• Key vendors for CIPL are the ISPs, OEMs and other local service providers. • Since there are multiple providers, the likely impact has been taken care off. • Adequate SLA / NDA are signed between the two interested parties to protect the Information / Confidentiality of the organization. • All information related to vendors/suppliers should be adequately secured. • Adherence to payment terms • Adherence to contractual agreements
5	Consultants / Subject Matter Experts	External	• CIPL hires Domain/Subject matter experts for specific requirement. • Adequate SLA / NDA's are signed between the two interested parties to protect the Information / Confidentiality of the organization.
6	Regulators / Government Agencies / Legal	External	• CIPL needs to fulfil the Regulatory requirements as per Company act and other appropriate relevant laws applicable to the organization • Data Protection Act, • Companies Act
7	Insurer	External	• Meeting policy requirements • Payment of premiums • Reporting changes in circumstances
8	Trade bodies / Associations	External	• Membership requirements • Meeting standards to which the organization • adheres • Provision of guidance
9	Bank and/or other finance providers	External	• Meeting repayment terms • Compliance with loan conditions

10	Neighbors / Owner	External	• No complaints relating in relation to:
			  • Noise
			  • Parking
			  • Health and safety
			  • Pollution
			  • Waste
			• Consideration to the neighbourhood/ owner when planning any changes to the company's operations.

11	Certification Bodies	External	• The certification body expects compliance to
			  • Applicable standard(s) that company has registered
			  • Any applicable legal or other requirements that

Formatted: Font: 10 pt

Sr. No.	Interested Party	Type	Information Security Expectations / Requirements
			the company has obligations for.

Formatted: Font: 10 pt

4.2.2 Interface and Dependencies

4.3 Determining the scope of the information security management system

CIPL has designed an ISMS framework that covers the entire CIPL / considering all the processes of the organization. However, the coverage of the ISMS is better defined in terms of the business units, locations and the services offered by the CIPL. Following are the various departments included under the scope of the ISMS:

- Marketing
- Practices
- Human Resources
- Talent Acquisition
- Project Management Office
- Academy
- Administration
- Information Technology
- Infrastructure Project Delivery
- Resourcing
- Managed IT
- Application Development
- Application Support
- Sales

Formatted: Font: 10 pt

- Project Management
- Center of Excellence – COE
- Corporate Quality
- Legal and Compliance

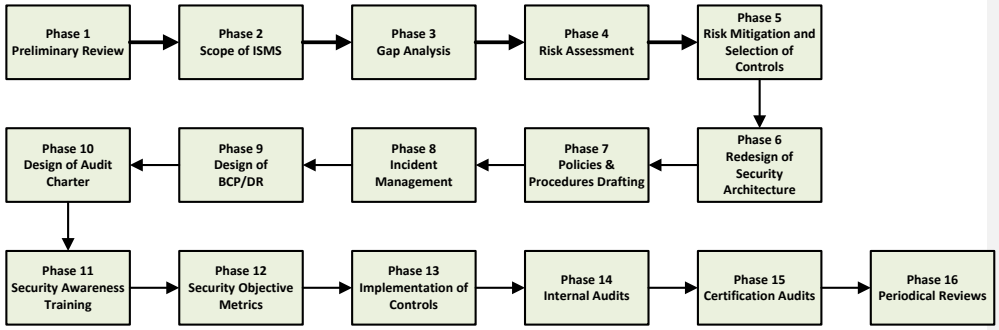
4.4 Information Security Management System

4.4.1 Standards, Guidelines, Models used adopted by CIPL

CIPL has developed its information security strategies based on the requirements of ISO 27001:2013 standard and the continual improvement approach as required by the various other ISO standards.

4.4.2 Framework for building ISMS

A framework for building the ISMS for CIPLcovering the above-mentioned location is as illustrated below



Formatted: Font: 10 pt

4.4.3 List of Processes incorporated in the Information Security Management System

4.4.3.1 System Processes

Sr. No.	Name of Process	Document Reference
1	Management Review Process	ISMS-L2-PR-CISO-01
2	Internal Audit Process	QMS-L2-PR-MR-02
3	Corrective Action Process	QMS-L2-PR-MR-03
4	Document Control Process	QMS-L2-PR-MR-04
5	Monitoring and Measurement Process	QMS-L2-PR-CISO-03
6	Customer Management Process	QMS-L2-PR-MR-06
7	Risk Assessment Process	ISMS-L2-PR-CISO-02
8	Change Management	QMS-L2-PR-MR-08
9	Business Continuity Process	ISMS-L2-PR-CISO-04
10	Human Resource Process	QMS-L2-PR-HR-01
11	Legal and Compliance Process	ISMS-L2-PR-CISO-05
12	Capacity Management Process	ISMS-L2-PR-CISO-06

4.4.3.2 Operations Processes

Sr. No.	Name of Process	Document Reference
1	Marketing Process	QMS-L3-PR-OPR-01
2	Practices Process	QMS-L3-PR-OPR-02
3	Talent Acquisition Process	QMS-L3-PR-OPR-03
4	Project Management Office Process	QMS-L3-PR-OPR-04
5	Academy Process	QMS-L3-PR-OPR-05
6	Administration Process	QMS-L3-PR-OPR-07
7	Information Technology Process	QMS-L3-PR-OPR-08
8	Managed IT Process	QMS-L3-PR-OPR-09
9	Resourcing Process	QMS-L3-PR-OPR-10
10	Infrastructure Project Delivery Process	QMS-L3-PR-OPR-11
11	Application Support Process	QMS-L3-PR-OPR-12
12	Sales Process	QMS-L3-PR-OPR-13
13	Project Management Process	QMS-L3-PR-OPR-14
14	Centre of Excellence – COE Process	QMS-L3-PR-OPR-15
15	Corporate Quality Process	QMS-L3-PR-OPR-16
16	Application Development Process	QMS-L3-PR-OPR-17

Formatted: Font: 10 pt

5. Leadership

5.1 Leadership and Commitment

5.1.1 General / Management Responsibilities

"CIPL is directed to establish aInformation 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."

The management of CIPL has provided evidence of its commitment to the establishment, implementation, operation, monitoring review, maintenance and improvement of the ISMS by doing the following:

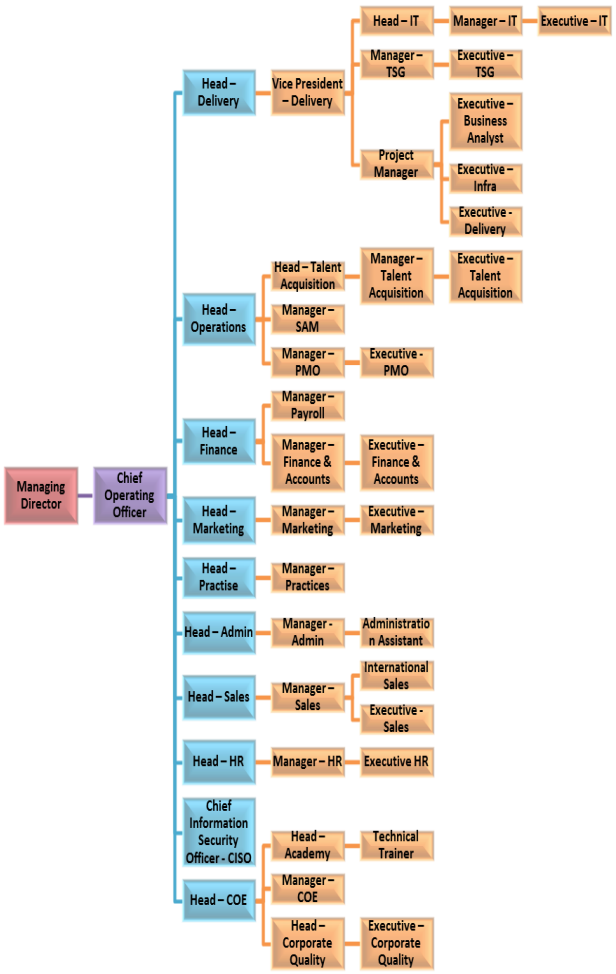
- Formulated and established a information Security Policy (Please refer to Information Security Policy.doc);
- Ensured that Security Objectives, plans are established and appropriate procedures are developed and communicated to all the employees;
- Established roles and responsibilities for the development and implementation of ISMS by formulating the necessary teams;
- Communicated to the organization the importance of Security, meeting Security Objectives and conforming to the Information Security Policy, its responsibilities under the law and the need for continual improvement;
- Provided sufficient resources to develop, implement, operate, review and maintain the ISMS;
- Has appointed a CISO and given the responsibility of continuously planning reviews and conducting management reviews of the ISMS with the participation of the Management so as to ensure continual improvement of the System. In the absence of CISO, any other member of ISMF or Deputy CISO shall coordinate the activities of CISO.
- Maintain all documents related to Information Security Management System.
- Reporting to Management on the performance of the Information Security Management System.
- Arranging internal audits.
- Follow up with respective Managers for closure of findings and ensuring compliances to the processes
- Ensure essential trainings are given to all concern team members
- Liasoning with certification agencies.
- Ensure security system is co-ordinated with all Managers & Senior Management continuously to monitor the activities by reviewing department-wise records to verify effective implementation of the system.
- Establish the Organization Structure and making necessary changes in it from time to time

5.1.2 Customer Focus

- Ensure that customer requirements and applicable legal requirements are determined, understood and met
- Determine and address customer satisfaction by identifying all possible risks which can affect conformity of CIPL
- Focus on enhancing customer satisfaction is maintained

Formatted: Font: 10 pt

5.1.3 Organization Chart



Formatted: Font: 10 pt

5.2 CIPL's Information Security Policy Statement

INFORMATION SECURITY STATEMENT:

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 will be assured*
- ***Integrity** of Information will be maintained*
- ***Availability of Information and Information Systems** will be met*
- ***Regulatory** and **Legislative r**equirements will be met*
- ***Business Continuity** planswill 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***
- ***User Guidelines stating Do's and Don'ts** related to usage of internet, email, computer system, and measures taken for data protection will be established*
- *All employees, **Senior Management to L1 level employee,** will be **responsible** for **implementing and adhering to information security policies** within their scope of deliverables.*

Mr. Javed Tapia

Managing Director

5.2.1 Communicating the Security Policy

- Top Management uses the Security Policy as a means of leading the organization towards improvement of its performance.
- Security Policy is communicated through electronic root messages to all employees and is displayed at salient locations within organization.
- Security Policy is presented on Intranet along with other relevant documents of ISMS
- Through training programs on ISMS, regular reviews of Company level Security Objectives, the Senior Management team ensures that members at every location / department:-

Formatted: Font: 10 pt

- **Understand the Security Policy**
- **Implement the Security Policy**
- **Maintain the Security Policy**

- All personnel are trained on Security and are informed that compliance with the policy is mandatory.
- All managers are directly responsible for implementing the policy and ensuring staff compliance in their respective departments.

5.3 Organizational Roles, Responsibilities and Authorities

Organization structure and responsibility authority defined and communicated through email and during trainings.

Please refer to "Roles and Responsibilities" document for details.

5.4 CISO

Clover Infotech Pvt. Ltd. has appointed Mr.Javed Tapia– MDas a member of management who, irrespective of other responsibilities:

a. Ensures that processes needed for the Information Security Management System are established implemented and maintained.
b. Reports to top management on the performance of the Information Security Management System and any need for improvement.
c. Ensures the promotion of awareness of customer requirements throughout CIPL.

The responsibility of a CISO shall include liaison with external parties on matters relating to the Information Security Management System.

Detailed responsibilities and Authorities of CISO are defined above at 5.3.

Mr. Javed Tapia– MDappoints Mr.Vikram Gite–AVP Delivery,as Chief Information Security Officer (CISO) with additional responsibility of Information Security Management System as described above at 5.3.

Mr. Javed Tapia – MD also appoints Mrs. Nisha Bandodkar – Head – Corporate Quality, as Deputy CISO.

Formatted: Font: 10 pt

6. Planning

6.1 Actions to address risks and opportunities

In order to manage information security, CIPL will adopt a risk-based approach. This approach mandates:

- The identification of all critical information assets in the scope.
- The identification of security vulnerabilities in these information assets.
- The identification of threats and threat probabilities that may result in exploitation of the vulnerabilities.
- The identification of the proper set of controls to protect these assets from the identified threats. Controls should also be identified in line with any client guidelines or contractual clauses on information security.
- The proper business continuity solutions to deal with loss of key assets processes, people, or physical premises.
- To periodically assess the risk in order to ensure it is being adequately managed, and previously identified risks are being addressed.

Refer to Risk Assessment Procedure for more details.

6.1.1 Statement of applicability

Statement of applicability (SOA) will map ISMS controls with documented and implemented processes of CIPL can be found in the document "Statement OfApplicability Version 2.3" dated 3rd September 2018. The statement has been prepared taking into account applicable control objectives implemented.

CIPL management has reviewed and approved the proposed residual risks and has given its authorization to implement and operate the ISMS.

6.2 Information Security Objectives and planning to achieve them

6.2.1 Information Security Objectives

CIPL intends to safe guard their assets involved in business by implementing standard controls like ISMS which are internationally accepted and tested for good result.The standards have helped achieve business objectives like effectiveness, efficiency, confidentiality, integrity, reliability, availability and Compliance. These objectives need to be measured by implementing certain processes or practices.

ISMF shall ensure that ISMS objectives, including those needed to meet requirements for products/services are established at relevant functions and levels within CIPL. The ISMS objectives identified are measurable and consistent with the ISMS policy as under:

S. No.	Parameter	Objective	Periodicity	Responsible Team
1	Average Minor Non-conformities per AUDIT Cycle (per department)	**<=5**	Every 6 months (Post Audit)	ISMS

Formatted: Font: 10 pt

S. No.	Parameter	Objective	Periodicity	Responsible Team
2	Internet Downtime (on Working days in working hours)	**>=99% availability**	Monthly	IT Team
3	Infected file status (new + still infected) count because of virus and spyware	**<=3**	Monthly	IT Team
4	Overall High priority Incidence Occurrence Rate Admin +Facilities IT HR(should include incidents related to POSH) Customer Delivery/Project	**<=5** **<=5** **<=5** **<=5**	Monthly	Admin IT HR
5	Customer Satisfaction on Internal infrastructure	**>=90%**	Every 6 months (Pre- Audit)	Support/ Delivery/ IT
6	Repetition of Audit Findings in next Internal Audit	**<=2**	Every 6 months (Post Audit)	ISMS
7	Count of residual risks	**<=10**	Yearly (Pre-audit)	ISMS
8	Full back up failures	**<=2 times**	Monthly	IT Team
9	Downtime due to power failure (during working hours)	**<=6 hours**	Monthly	Admin team
10	Number of employees relieved/ terminated without execution of HR Exit check list	**=100% compliance**	Quarterly	HR team
11	Background Verification for all employees	**100%**	Monthly	HR Team

ISMF shall ensure that above mentioned objectives measurement data shall be collected on periodical basis and it shall be analyzed against set objectives.

Please Refer to Measurement Metric Report.

6.2.2 Security Awareness Program

Information security management system will continue to grow and maintain itself only if the people of CIPL are continuously vigilant and are able to absorb information security principles in their work culture.

In accordance with this statement, it is essential for the company to implement security awareness initiatives at all levels of CIPL, including senior management, middle management, team leaders, and head of the departments, support staff, and any third parties.

The information security awareness sessions will be an ongoing initiative which will ensure that all the employees and contractors are aware of the information security policies that are relevant to them. In addition, all the procedures, guidelines, and information security best practices in conjunction with other laws, regulations, and management best practices as adopted by the company.

Formatted: Font: 10 pt

6.2.3 Security Metrics and Measurement

In addition to maintaining the information security management system, it is imperative to monitor and measure its ongoing efforts and results as well. There will be a procedure to maintain metrics to beimplemented in the organization. The procedure will also identify techniques for implementing and reviewing measurements of the identified metrics. The inputs and outputs to the measurements will be reviewed on a regular basis in line with the procedure.

6.2.4 Legal or Regulatory Requirements

The company shall protect its sensitive information from unauthorized disclosure. The primary laws and regulations with which it does this are as follows:

- 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

Formatted: Font: 10 pt

- The Payment of Bonus (Amendment) Ordinance, 2007
- Maharashtra Shops and Establishments (Regulation of Employment and Conditions of Service) Act, 2017

6.2.5 Review

The Corporate Information Security Policy, as well as the other security policies must be periodically reviewed. This review will happen under the following circumstances:

- Once every 12 months irrespective any changes in Business Environment
- If there is a significant change in the technologies in use by the company
- If there is a significant change in the external threat environment, which mandates a review of the risk profile
- If there is a significant change in client requirements/guidelines for information security

7. Support

7.1 Resources

CIPL has determined and provided the resources to do the following on a continuous and ongoing basis:

- Establish, implement, operate and maintain the ISMS (Please refer to Information Security Policy.doc)
- Ensure that the information security procedures support the business requirements and commitments
- Identify and address legal and regulatory requirements and contractual security obligations
- Maintain adequate security by correctly implementing and applying all the identified controls. Refer to Statement of Applicability.
- Conduct reviews twice in a year for improving the effectiveness of the ISMS

7.2 Competence

Determined the necessary competence for personnel performing work affecting security and same is recorded as per designation /post in Competency Matrix.

Please Refer to Competency Matrix (iConnect Report):

7.3 Awareness

The behavioral/ skill based training needs are identified to satisfy the product or service requirements and the identified trainings are planned and documented in the Training Calendar.

Personnel are made aware of the relevance and importance of their activities which are communicated while training and how they contribute to the achievement of the IS objectives.

Formatted: Font: 10 pt

Appropriate records of education, training, skills and experience are identified and recorded.

Training is given to concerned resources who are involved in closure of Corrective actions activities to maintain the status of Information Security Management System.

The above activities will be performed on an ongoing basis taking into account any changes to

- Organization
- Technology
- Business objectives and processes
- External events such as changes to legal and regulatory requirements and changes in social climate.

Please refer to HR Training Calendar

Formatted: Font: 10 pt

7.4 Communication

Internal as well as external communication will be as follows:

Sr. No.	Department / Policy / Procedure	Action / Trigger	Internal / External	Relevant Party
1	Information Security	Updation of Policy	Internal	All Teams / CISO
2	Risk Assessment	Addition / Updation / Deletion of Risks	Internal	All Teams / CISO
3	Asset Management	Addition / Updation / Disposal of Assets	Internal	All Teams / CISO
4	Access Controls Management	Addition / Updation / Deletion of Resources	Internal	HR / Admin / IT Team
5	Physical and Environmental	Incident	Internal / External	HR / Admin / IT / Third Party
6	Password	New / Change / Reset	Internal	Employee / IT Third Party
7	Incident Management	IT / Non IT Incident	Internal / External	HR / Admin / IT / Third Party
8	Internal Audit	Audit Schedule / Plan	Internal	All Teams / CISO
9	Human Resource	Resource Request / On Boarding / Separation	Internal / External	HR / Admin / IT Team
10	Acceptable usage	Incident	Internal / External	HR / Admin / IT / Third Party
11	Network	Addition / Updation / Deletion / Incident related to Network	Internal / External	IT / Third Party
12	Data Centre	Addition / Updation / Disposal of H/W S/W	Internal / External	IT / Admin / Third Party
13	Internet	Addition / Updation / Deletion / Incident related to Internet	Internal / External	IT / Admin / Third Party
14	Anti-Virus	Addition / Updation / Deletion / Incident related to Anti-Virus	Internal / External	IT / Third Party
15	Backup	Addition / Updation / Deletion / Incident related to Backups	Internal	IT / All Teams
16	Patch Management	Addition / Updation /	Internal /	IT / All Teams / Third

Formatted: Font: 10 pt

Sr. No.	Department / Policy / Procedure	Action / Trigger	Internal / External	Relevant Party
		Deletion / Incident related to Patches	External	Party
17	Change Management	Change Request	Internal / External	IT / Admin / Third Party
18	Desktop	New / Up-gradation / Release Request	Internal	IT / Admin
19	Business Continuity	Business Continuity Incident	Internal / External	IT / HR / Admin / Third Party
20	Procurement of H/W and S/W	Procurement Request for H/W S/W	Internal / External	IT / Admin / Third Party
21	Management Review	Periodical Review / Critical Incident / Specific Request	Internal	All Teams / CISO
22	Corrective Action	Internal Audit – Non Compliance / Observation / External Requirements	Internal / External	All Teams / CISO
23	Software / Product Development	Requirements / Design / Coding / Release Notes	Internal / External	Software / Product Team
24	Business Developments	Request for Proposal (RFP), Letter of Acceptance / Agreement / Invoices / Payment	Internal / External	Business Development Team

Mode of communication:

- Phones
- Letters
- Email
- Meetings supported by Minutes of Meeting
- Conference calls followed up with email / Minutes of Meeting

7.5 Documented Information

7.5.1 General

The Information Security Management System is documented and it includes:

- Information Security Manual - Level 01
- Documents needed by CIPL to ensure the effective planning, operation and control of its processes and – Level 02 (System Procedures).
- Documents needed by CIPL to ensure the effective planning, operation and control of its processes and – Level 03 (Operations Procedures).

Formatted: Font: 10 pt

- Forms, Guidelines, Checklist and Templates as required by the respective procedures – Level 04 (Templates)
- Documents needed by CIPL to ensure the effective planning, operation and control of its processes and – Level 05 (Policies).

The levels of documents are as follows:

Sr. No.	Description	Level
1	Information Security Management System Manual	Level 01
2	All System Procedure Documents (Procedures)	Level 02
3	All Operational Procedure Documents (Procedures)	Level 03
4	Forms, Guidelines, Checklist and Templates as required by the respective procedures	Level 04
5	All Policy Documents (Policies)	Level 05

7.5.2 Creating and Updating

Following is the procedure followed to control the documents and to maintain the Information Security Management System:

- Documents required by the Information Security Management System are maintained and controlled in the Master List of Documents.

  List of QM Records: Master list of Documents.

- Following controls are followed for documents control and as per the standard requirements:
  - Approval of documents for adequacy prior to issue
    All documents are approved and released prior to use and Master List of documents prepared with approving authority mentioned in same list as Master list of Documents
  - Review and re-approve of documents
    All documents review and re approval is maintained in Master List of documents and the same is updated regularly whenever review or re approval takes place. The approval details are mentioned in the document itself.
  - Changes and the current revision status of documents are identified in document itself by revision number and date of revision.
  - Confirming relevant versions of applicable documents are available at points of use. The relevant version will be controlled by version number and version date.

    For issue and revision control following method is adopted:
    - For the first draft issue documents the version status is 0.0.
    - For the first release document after review of the draft version status is 1.0
    - Whenever there is any minor change in particular document the version number is raised as 1.1, 1.2, 1.3 etc.
    - Whenever there is any major change in particular document the version number is raised as 2.0, 3.0 etc.
  - Documents legibility and identifiable.

Formatted: Font: 10 pt

Document status is identified by putting a mark on each and every page of the Level 1, 2, 3 and Cover page of Level 4.

- Master copy– in editable format
- Control copy – in .pdf format
- Obsolete copy – in .pdf format

- Unintended use of obsolete documents, and suitable identification

  All obsolete copies will be stamped / water marked, maintained separately and retained as per the requirement.

7.5.3 Control of Documented Information

7.5.3.1 Forms and Format Numbering

The following method is followed for Document numbering and identification for forms, registers, reports and format:

ZZZ-LX-XX-AAA-99 <Name of the document>

ZZZ – Represent System Type (System Type: ISMS – Information Security Management System)
LX – Represents Level type of Document (Level Type: L1/L2/L3/L4)
XX – Represents the document type (document types: FR- Forms, LS-Lists, RG-registers, ML-Manual, PR-Procedure, CD-Coding Standard, CK-Checklist, GD-Guidelines)
AAA – Represents the policy/procedure document name/number (HR-Human Resource, ADM-Administration, OPR-Operations, TA-Talent Acquisition, MKT-Marketing, PRT-Practices, MR-Management Representative, CISO – Chief Information Security Officer, PMO-Project Management Office, IFD-Infrastructure Delivery, SYS-System, and IT-Information Technology, SDLC-Software Development Life Cycle, RES-Resourcing, ADS-Application Delivery Support, ADD-Application Development Delivery, SAL-Sales, PM-Project Management, COE-Center of Excellence, CQ-Corporate Quality, ACD - Academy)
99 – Serial number
<name of the document>

For example: ISMS-L1-ML-CISO-01 stands for Information Security Manual of Level Type L1 of Document Type ML (Manual) of CISO having serial number 01.

7.5.3.2 Control of Documented Information

Following is the procedure followed to control the records and maintain the ISMS System:

- Records are established and maintained to provide evidence of conformity to requirements and of the effective operation of the Information Security Management System.
- Record's keeping is made in such a way that, they remain legible, readily identifiable and retrievable.
- List of records is prepared and followed for defined controls required for identification, storage, protection, retrieval, retention time and disposition of records. i.e. Master list of documents

Formatted: Font: 10 pt

- Hard copy and Soft copy records are controlled and recorded in list of records
- The soft copy - Project files/ folders are named as follows:
  <Project Name>_<Level 1_……_Level n>
  The Project Name will be followed by Levels 1 to n, which denote the various levels into which the project will be divided for simplicity. The hierarchy (number of levels) will have to be specified in the Project Plan.
- All documents are maintained by Project Manager / Project Superintendent
- All project specific files and documents will be stored using the above naming convention
  Under Documents following Paths are created and documents are stored
  - \Architecture
  - \Design
  - \Functional Specification
  - \Testing
- All Obsolete documents are archived and Records are updated in Master List Document

Please refer Document Control Procedure - QMS-L2-PR-MR-05 for more details

7.5.3.3 Classification of Documents

All documentation covered by this procedure shall adhere to the following:-

- It is uniquely referenced, legible and readily identifiable.
- Documentation is protectively marked with the requisite security classification when not for general distribution. It is the responsibility of the owner of the data to accord it the relevant security classification. The various classes of security classification to be applied to documents at Clover as follows:-
  - Unclassified – Unrestricted viewing. Examples include press releases, general policy documents of the company that are available on the company's website.
  - Company Circulation – These documents are for internal use only and the contents should not be shared by any outsider. Examples include the policies and procedures adopted by Clover, market survey reports and other commercial information.
  - Confidential – These documents are highly sensitive and examples include reports of audits of customers, internal policy documents the exposure of which shall cause embarrassment and serious loss of business to Clover.
- It is made readily available to all personnel having legitimate access rights, at all locations where the subject operations are performed.
- It is restricted sufficiently to prevent unauthorized access.
- Documentation is periodically reviewed and revised as necessary
- It is maintained under version control, including issue and revision dates and, where relevant, the dates for review.
- Documentation is withdrawn promptly when obsolete or superseded.
- It is identified and retained when obsolete but required for legal or knowledge preservation.

Formatted: Font: 10 pt

8. Operations

8.1 Operations Planning and Control

8.1.1 Preliminary Review and planning

ISMF team initially reviews the current status of documentation and plan activities for operations. Also ISMF team plans implementation of Information Security Management System.

8.1.2 Identification of Scope of ISMS

ISMF team reviews details and define scope of ISMS to be implemented for CIPL.

8.1.3 Gap Analysis

ISMF team reviews details and identify gaps based on the ISO 27001:2013 standard to be implemented. ISMF team plans activities to fill up these gaps and prepare project plan.

8.1.4 Risk Assessment

ISMF team assesses the probable risks associated with various operations carried out by all departments. These risks are noted and analyzes further for taking appropriate action.

8.1.5 Risk Mitigation and Selection of Controls

ISMF team analyzes the risks and prepares Mitigation Plan to avoid the occurrences of these risks. Appropriate controls are identified and implemented to mitigate risks.

8.1.6 Redesign of Security Architecture

ISMF team redesign Security Architecture based on identified risks, identified controls and mitigation plan to take care of Risks

8.1.7 Policies and Procedures Drafting

ISMF team set appropriate policies to set operations and design procedures for smooth operations of the all the departments in CIPL

8.1.8 Incident Management

ISMF team set incident management policy / procedure to address to various incidents happening in CIPL and take corrective actions promptly to resolve the same.

8.1.9 Design of BCP / DRP

ISMF team prepares Business Continuity and Disaster Recovery planning activities for smooth operations

Formatted: Font: 10 pt

of CIPL.

8.1.10 Design of Audit Charter

ISMF team prepares Audit Charter (plans) to review the operations periodically to verify set processes for its compliances and preventive activities. Audit findings are taken seriously and close the same at the earliest for better operations.

8.1.11 Security Awareness Program

ISMF team prepares training schedule and impart training to all employees. New joinees are given training during the induction program. Periodical reviews are taken to check the competence of the resources for respective areas of operations.

8.1.12 Security Metrics

ISMF team defines various security metrics to measure the effectiveness of processes and take corrective actions.

8.1.13 Implementation of Controls

ISMF team implements various security controls to avoid any non-compliances. These controls are closely monitored for better performance.

8.1.14 Internal Audits

ISMF team conducts internal audits as per scheduled plans and identifies non compliances for operations processes. Corrective actions are planned based on the non-compliances / observations to fix the concern.

8.1.15 Management Reviews

CIPL management reviews the operations periodically to see the progress of ISMS and take corrective actions to meet the requirements of ISMS.

8.2 Information Security Risk Assessment

Risks are assessed once in a six months and also if any major change takes place in the Information Security Management System. Corrective controls are established to “Reduce Risks” specific risks which exceeds limit.

These controls would either be to:

- Reduce the probability of occurrence of the threat
- Reduce the severity of the vulnerability
- Reduce the impact of the incident scenario

Formatted: Font: 10 pt

8.3 Information Security Risk Treatment

8.3.1 Risk Management Decision

After identifying the risks is to identify and evaluate the most appropriate action of how to deal with the risk. There are following possible actions for risk management decision

- Reduce
- Accept

Reduce Risk:

To reduce the assessed risks, appropriate and justified controls should be identified and selected. The aim of control selection is to reduce risk to a level, which is acceptable to CIPL.

Accept Risk:

Accept Risk is the conscious decision to accept the risk. When no further controls can be applied to reduce the risks, a decision needs to be made on how to deal with them. This decision is to accept risk.The management shall consider the following points to arrive at the risk acceptance criteria.

Different classes of risk, e.g. risks that could result in non-compliance with regulations or laws may not be accepted, while acceptance of high risks may be allowed if this is specified as a contractual requirement.

- Requirements for future additional treatment, e.g. a risk may be accepted if there is approval and commitment to take action to reduce it to an acceptable level within a defined time period

Refer to Risk Management Procedure for more details.

Formatted: Font: 10 pt

9. Performance Evaluation

9.1 Monitoring, Measurement, Analysis and Evaluation

9.1.1 Monitoring and Measurement

The CIPL is committed to defining, planning and implementing appropriate and effective measuring/monitoring activities, needed to assure that services provided conform to customer requirements and achieve improvement.

9.1.2 Customer satisfaction

The CIPL monitors and reviews information sought/received to determine customer perceptions as to whether CIPL has met their requirements. Such information may be received by all/any of the following methods:

- General day-to-day Customer communication.
- Customer Feedback on milestones
  - Need Analysis
  - Delivery
  - Issue / Problem Management
- Monitoring and Measurement.

The PM/ PL is responsible for ensuring appropriate implementation and follow-ups for customer feedbacks.

Refer to Customer Feedback

9.1.3 Monitoring and measurement of processes

CIPL has implemented suitable methods of measuring/monitoring all processes necessary to meet customer requirements. Such methods include:

- Appropriate documented operating procedures required to be followed.
- Internal Audits.
- Final recorded security checks on each customer contract.

These methods shall serve to confirm continuing ability to meet customer requirements.

Refer to Measurement Metric Report

Refer to Internal Audit Summary Report

9.1.4 Monitoring and measurement

Formatted: Font: 10 pt

The CIPL teams are monitoring their information assets based on predefined metrics and record control performance data. These reports are analysed to identify and highlight the root-cause of metric performance or lack thereof.

The repository of the reported information security incidents and weaknesses are also analysed and the data used for evaluating the effectiveness. The root-cause analysis for reported security incidents are also maintained in the incident register. An attempt also made to correlate reported incidents and weaknesses back to the ineffectiveness of implemented controls.

Audit findings, if any, during the defined period are also considered as indicators of the effectiveness of security controls.

VAPT reports are taken once in six months and corrective actions needs to be taken to close the observations to minimize risks.

All metrics identified 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 periodicities for individual metrics tend to vary depending on the requirements of the business and consequently the ISMS. For a snapshot of the status of effectiveness of controls, the most recent data for each metric/control shall be considered.

The first six 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.

Monthly datashall be evaluated against the baseline by comparing the data of the subsequent months. The objective of this activity is to strive towards improving or increasing the baselines requirements to ensure that security control effectiveness is constantly increasing.

Measurement of Effectiveness of Security Controls:

It is impractical to attempt monitoring all of the applicable controls of the standard and hence the monitoring activities will focus on a few critical controls which are identified as critical to CIPL operations and subsequently approved by the Group Head. The effectiveness of only these controls will be measured.

CIPL identifies security controls that are most critical to their operations and establish metrics for these. The performance of the metric serves as a measure of the effectiveness of those implemented controls.

All information security incidents, weaknesses/vulnerabilities, non-conformities and metric performance data are reported periodically to the Management.

It is reasonable to assume that an incident/weakness/non-performance of identified metrics have resulted from inadequate or ineffective implementation of a control or a group of controls belonging to one or various security domains) or a faulty implementation.

Formatted: Font: 10 pt

The list of controls/metrics to be monitored is analysed and more controls added if found effective and feasible.

Following are the processes implemented for monitoring, measuring, analyzing and evaluating organization's policies and processes performance,

- Helpdesk
- Periodical MIS
- Incident management
- Service level management
- Change management
- Vulnerability assessment
- Information security management system
- Periodical review by internal audits
- Management review
- Continuous improvement

Refer to Measurement Metric Report

9.1.5 Analysis and Evaluation

CIPL shall determine, collect and analyze appropriate data to demonstrate the suitability and effectiveness of the information security management system and to evaluate where continual improvement of the effectiveness of the information security management system can be made. This shall include data generated as a result of monitoring and measurement and from other relevant sources.

The analysis of data shall provide information relating to

- Customer satisfaction
- Conformity to product requirements
- Characteristics and trends of processes and products including opportunities for preventive action
- Suppliers

Refer to Measurement Metric Report

9.2 Internal Audit

Successful implementation of the IS System is directly related to the effectiveness of its internal auditing procedure. The top management is responsible for approving the audit programme, which is maintained, by the CISO.

The following procedure is followed for conducting internal audit:

- CISO has the responsibility to plan and organize the Internal IS Audits.
- Internal IS Audits are conducted once in Six Months.

Formatted: Font: 10 pt

- Internal IS Audits are conducted according to the plan.

Refer to Internal Audit Plan

CISO informs three days in advance to concerned personnel through internal IS Audit Schedule, with the details of the following:

- Audit Function
- Scope of the Audit
- Duration
- Date and Time
- Auditee/s and Auditor/s

Refer to Internal Audit Schedule

- Auditors are independent of the functions to be audited.
- Auditors are chosen from the List of Trained Internal IS System Auditors.

Refer to List of Internal Auditors

All Internal/External auditors' records are maintained separately. Information Security Management System – Manual and ISO 27001:2013 Standard are the basis for audit. Auditor's observations are recorded in Audit observation report and on the basis of this report; the non-conformities are identified and recorded in the Audit non-conformities.

Refer to Internal Audit Report

Refer to Internal Audit Summary Report

Auditee responsible acknowledges the non-conformity and recommends the proposed corrective action/s along with completion date. Based on corrective action, required documents are identified. If preventive action is required, the same is identified by the Auditee.

Auditors submit the non-conformance report duly acknowledged by the Auditee to the CISO.

The copy of the Non-conformance report of the audit is provided to Auditee.

CISO organizes for the follow-up audit to verify the implementation of the proposed corrective action taken and to verify the effectiveness of implementation of corrective/ action. If these corrective actions taken are found satisfactory then the CISO closes the Non-conformities.

Based on the number of non-conformities, CISO prepares a summary report having number of non-conformities found against ISO 27001:2013 Clause number.

Refer to Internal Audit Summary Report

The CISO is responsible to maintain all records pertaining to Internal Audits for a minimum of three years.

Formatted: Font: 10 pt

9.3 Management Review

9.3.1 General

The Management reviews CIPL's information security management system, after every six months. This is to ensure its continuing suitability, adequacy and effectiveness. These reviews are conducted with all concerned personnel.

Reports and records of MRM will be maintained by CISO.

This review will include assessing opportunities for improvement and the need for changes to the information security management system, including the information security policy and IS objectives.

9.3.2 Review Input

Before conducting management review meeting CISO will prepare MRM agenda covering following points as a MRM inputs:

- Status of actions from previous Management Review
- Changes in external and internal issues that are relevant to the Information Security Management System
- Feedback from the Information Security performance, including trends in
    - Non-Conformities and Corrective actions
    - Monitoring and Measurement results
    - Audit results
    - Fulfillment of Information Security objectives
- Feedback from Interested Parties
- Result of Risk Assessment and status of Risk Treatment Plan
- Opportunities for Continual Improvements

Other requirements are identified and circulated as and when necessary.

Refer to MRM Agenda

9.3.3 Review Output

After management review meeting the management review is recorded in minutes of MRM with decisions and actions leading towards:

- Improvement of the effectiveness of the IS management system and its processes.
- Improvement of product related to customer requirements.
- Resource needs.

Refer to Minutes of MRM

Formatted: Font: 10 pt

10. Improvement

10.1 Non-Conformity and Corrective Actions

10.1.1 Non-Conformity

CIPL has ensured that product which does not conform to product requirements is identified and controlled to prevent its unintended use or delivery. The controls and related responsibilities and authorities for dealing with nonconforming product shall be defined in a documented procedure.

CIPL will deal with nonconforming product by one or more of the following ways:

- by taking action to eliminate the detected nonconformity,
- by authorizing its use, release or acceptance under concession by a relevant authority and where applicable by the customer,
- by taking action to preclude its original intended use or application.

The concerned personnel informs the non-conformities and any subsequent actions taken, including any concessions obtained through the records maintained in the Internal Audit Report.

When nonconforming product is corrected it shall be subject to re-verification to demonstrate conformity to the requirements.

Refer to Internal Audit Report

When nonconforming product is detected after delivery or use has started, CIPL shall take action appropriate to the effects, or potential effects, of the nonconformity.

10.1.2 Corrective action

CIPLis committed to taking appropriate corrective action to eliminate the cause of non- conformities to prevent recurrence whenever practical/possible. Such action shall be appropriate to the impact of the problems encountered.

The CISO on a regular basis, just prior to Management Review, undertakes a review of all non-conformities, as documented / presented in accordance with procedure and data. This review serves to ensure that actions (previously) taken have proved to be effective, possible reoccurring trends/ weaknesses may be identified. Such review provides an opportunity to review if further actions are required.

This review is documented and presented to top management (normally at Management Review meetings) with CISO's findings/observations/suggestions/actions as appropriate.

10.2 Continual Improvement

By means of the IS policy/objectives, audit results, analysis of data, corrective action, management review etc. the Organization is committed to the process of continual improvement.

Formatted: Font: 10 pt

Need for preventive action are discussed with top management and documented accordingly with appropriate actions to be taken. The CISO is required to follow up, to verify that such actions have been taken and that they have been found to be effective.

The Non-Conformance records can also be used to document potential problems/weaknesses as a means of communicating same to CISO.

Refer toAreas of Continual Improvement Register

Formatted: Font: 10 pt

….END OF INFORMATION SECURITY MANUAL – LEVEL 01….

Formatted: Font: 10 pt