# IRIS BUSINESS SERVICES LIMITED




# Information Security Procedures/Process/Guidelines

Version 1.6

**APRIL – 2024**

**Document Information**

| | | | |
|---|---|---|---|
| **Document Name** | Information Security Management Procedure/Standards/Guidelines | **Version** | 1.6 |
| **Date Created** | 28 August 2017 | **Released Date** | 11th April 2024 |

| | |
|---|---|
| **Document No.** | ISMS 03 |
| **Classification** | Internal |
| **Prepared By** | Akshay Rane |
| **Reviewed By** | Mahesh Tilave |
| **Approved By** | P K X Thomas |

**Distribution:** To all employees and relevant consultants, contractors, vendors and third parties of the IBSL.

**Review history:**

| Sr.No | Author | Date | Review details | Version Number |
|---|---|---|---|---|
| 1 | CISO | March 2018 | No Change required | Ver 1.0 |
| 2 | CISO | March 2018 | Change in team members | Ver. 1.1 |
| 3 | CISO | March 2019 | Annual Review (No change) | Ver. 1.1 |
| 4 | CISO | September 2020 | Annual Review | Ver 1.2 |
| 5 | CISO | September 2021 | Annual Review | Ver 1.3 |
| 6 | CTO | August 2022 | Annual Review | Ver 1.4 |
| 7 | CTO | April 2023 | Annual Review | Ver 1.5 |
| 8 | CTO | April 2024 | Change in 18.1.4. Privacy and protection of personally identifiable information | Ver 1.6 |

**Summary of changes from the previous release**

| Sr. No. | Version | Brief Description of the change(s) made |
|---|---|---|
| 1 | 1.0 | Initial release |
| 2 | 1.1 | Change in team members |
| 3 | 1.2 | Changes according to change in scope from product specific to enterprise level certification<br>Added 6.2.3 Information Security Measures for remote working during Pandemic period<br>Added 11.1.7 Physical security Measures during Pandemic period<br>Change in process owners |
| 4 | 1.3 | Updated Inventory of Assets & Disposal of Media<br>Updated Vulnerability Management<br>Added Patch Management |
| 5 | 1.4 | Annual Review |
| 6 | 1.5 | Annual Review |
| 7 | 1.6 | Added “2.Data received via email, whether PII or Non-PII, for debugging or troubleshooting purposes from client, is promptly and securely deleted :-Team Leader” in 18.1.4. Privacy and protection of personally identifiable information |

# Table of Contents

## Contents

**5. INFORMATION SECURITY PROCEDURE DOCUMENT ..... 9**

5.1.1 Policies for Information Security ..... 9

5.1.2 Review and Approval ..... 9

**6.0 ORGANIZATION OF INFORMATION SECURITY ..... 10**

**6.1 INTERNAL ORGANIZATION: ..... 11**

6.1.1 Information Security Roles and Responsibilities ..... 13

6.1.2 Segregation of Duties ..... 15

6.1.3 Contact with Authorities ..... 16

6.1.4 Contact with Special Interest Groups (Support from End users) ..... 16

6.1.5 Information Security in Project Management ..... 17

**6.2 MOBILE DEVICES AND TELEWORKING ..... 18**

6.2.1 & 6.2.2 Mobile Computing & Teleworking ..... 18

6.2.3 Information Security Measures for remote working during Pandemic period ..... 18

**7.0 HUMAN RESOURCE SECURITY PROCEDURE**
**7.1 PRIOR TO EMPLOYMENT ..... 21**

7.1.1 Screening ..... 21

7.1.2 Terms and conditions of employment ..... 21

**7.2 DURING EMPLOYMENT ..... 23**

7.2.1 Management responsibilities ..... 23

7.2.2 Information security awareness, education and training ..... 23

7.2.3 Disciplinary Process ..... 24

**7.3 TERMINATION AND CHANGE OF EMPLOYMENT ..... 25**

**7.3.1 TERMINATION RESPONSIBILITIES ..... 26**

**8 ASSET MANAGEMENT PROCEDURE ..... 27**

8.1 Responsibility for Assets ..... 27

8.1.1 Inventory of assets ..... 27

8.1.2 Ownership of Assets ..... 28

8.1.3 Acceptable use of assets ..... 28

8.1.4 Return of Assets ..... 30

**8.2 INFORMATION CLASSIFICATION ..... 31**

8.2.1 Classification of information ..... 31

8.2.2 Labeling of information ..... 32

8.2.3 Handling of assets ..... 32

**8.3 MEDIA HANDLING ..... 33**

8.3.1 Management of removable media ..... 33
8.3.2 Disposal of media ..... 33
8.3.3 Physical media transfer ..... 34
**9 ACCESS CONTROL PROCEDURE ..... 35**
9.1 Business Requirement for Access Controls ..... 35
9.1.1 Access control policy ..... 35
9.2 User Access Management ..... 37
9.2.1 User registration and deregistration process ..... 37
9.2.2 Use access provisioning ..... 38
9.2.3 Management of privileged access rights ..... 39
9.2.4 Management of secret authentication information of users ..... 39
9.2.5 Review of user access rights ..... 39
9.2.6 Removal or adjustment of user access rights ..... 40
**9.3 USER RESPONSIBILITIES ..... 42**
**9.3.1 USE OF SECRET AUTHENTICATION CONTROL ..... 43**
**9.4 SYSTEM AND APPLICATION ACCESS CONTROL ..... 45**
**9.4.1 INFORMATION ACCESS RESTRICTION ..... 46**
9.4.2 Secure logon procedures ..... 46
9.4.3 Password management system ..... 46
9.4.4 Use of privileged utility programs ..... 47
9.4.5 Access control to program source code ..... 47
**10 CRYPTOGRAPHY ..... 49**
10.1 Cryptographic Controls ..... 49
10.1.1 Policy on the use of cryptographic controls ..... 49
10.1.2 Key Management ..... 50
**11 PHYSICAL AND ENVIRONMENTAL SECURITY ..... 53**
11.1 Secure Areas ..... 53
11.1.1 Physical security perimeters ..... 53
11.1.2 Physical Entry Controls ..... 53
11.1.3 Securing Offices, Rooms and Facilities ..... 54
11.1.4 Protecting Against External and Environmental Threats ..... 54
11.1.5 Working in Secure Areas ..... 54
11.1.6 Delivery and Loading areas ..... 55
11.1.7 Physical security Measures during Pandemic period ..... 55
11.2 Equipment security ..... 56
11.2.1 Equipment siting and protection ..... 56

11.2.2 Supporting utilities ..... 56
11.2.3 Cabling security ..... 56
11.2.4 Equipment maintenance ..... 57
11.2.5 Removal of assets ..... 57
11.2.6 Security of equipment and assets off premises ..... 57
11.2.7 Secure disposal of reuse of equipment ..... 58
11.2.8 Unattended user equipment ..... 58
11.2.9 Clear desk and clear screen policy ..... 58
**12 OPERATIONS SECURITY MANAGEMENT ..... 60**
**12.1 OPERATIONAL PROCEDURES AND RESPONSIBILITIES ..... 61**
**12.1.1 DOCUMENTED OPERATING PROCEDURES ..... 62**
**12.1.2 CHANGE MANAGEMENT ..... 63**
**12.1.3 CAPACITY MANAGEMENT ..... 64**
12.2 Protection against Malwares ..... 64
12.2.1 Controls against Malicious Code / Malwares ..... 64
12.3 Backup and Retention/Archival ..... 65
12.3.1 Information backup ..... 65
12.4 Logging and Monitoring ..... 65
12.4.1 Event logging ..... 65
12.4.2 Protection of log information ..... 65
12.4.3 Administrator and operator logs ..... 66
12.4.4 Clock synchronization ..... 66
12.5 Control of Operational Software ..... 66
12.5.1 Installation of software on operational systems ..... 66
12.6 Technical Vulnerability Management ..... 67
12.6.1 Management of technical vulnerabilities - Application Security ..... 67
12.6.2 Restrictions on software installation ..... 68
12.6.3 Patch Management ..... 68
12.7 Information Systems Audit Consideration ..... 69
12.7.1 Information systems audit controls ..... 69
**13 COMMUNICATIONS SECURITY PROCEDURE ..... 70**
13.1 Network security management ..... 70
13.1.1 Network Controls ..... 70
13.1.2 Security of network services ..... 70
13.1.3 Segregation in networks ..... 71
13.2 Information transfer ..... 71
13.2.1 Information transfer policies and procedures ..... 71

13.2.2 Agreements on information transfer....72
13.2.3 Electronic Messaging & Instant Messaging....72
13.2.4 Confidentiality or non-disclosure agreements....72
14 **SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE PROCEDURE.... 73**
14.1 Security Requirement of Information Systems....73
14.1.1 Information security requirement analysis....73
14.1.2 Securing application services on public networks....73
14.1.3 Protecting application services transactions....73
14.2 Security in development and support process....73
14.2.1 Secure deployment policy....74
14.2.2 System change control procedures....74
14.2.3 Technical review of applications after operating platform....74
14.2.4 Restriction on changes to software packages....75
14.2.5 Secure system engineering principles....75
14.2.6 Secure development environment....76
14.2.7 Outsourced Development....76
14.2.8 System Security Testing....76
14.2.9 System Acceptance Testing....76
14.3 Test Data....77
14.3.1 Protection of test data....77
15 **SUPPLIER RELATIONSHIPS....78**
15.1 Information Security in Supplier Relationships....78
15.1.1 Information security policy for supplier relationships....78
15.1.2 Addressing security within supplier agreements....78
15.1.3 Information and communication technology supply chain....79
15.2 Supplier Service Delivery Management....79
15.2.1 Monitoring and review of supplier services....79
15.2.2 Managing changes to supplier services....79
16 **INFORMATION SECURITY INCIDENT MANAGEMENT....81**
16.1 Management of Information Security Incidents and Improvements....81
16.1.1 Responsibilities and procedures....81
16.1.2 Reporting information security events....81
16.1.3 Reporting information security weaknesses....81
16.1.4 Assessment and decision on information security events....82
16.1.5 Response to information security incidents....82
16.1.6 Learning from information security incidents....83

16.1.7 Collection of Evidence ..... 83
17 **INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT 84**
17.1 Information Security Continuity ..... 84
17.1.1 Planning information security continuity ..... 84
17.1.2 Implementing information security continuity ..... 84
17.1.3 Verify, review and evaluate information security continuity ..... 85
17.2 Redundancies ..... 85
17.2.1 Availability of information processing facilities ..... 85
18 **COMPLIANCE ..... 86**
18.1 Compliance with Legal and Regulatory Requirements ..... 86
18.1.1 Identification of applicable legislation and contractual requirements ..... 86
18.1.2 Intellectual property rights (IPR) ..... 86
18.1.3 Protection of Organizational Records ..... 87
18.1.4 Privacy and protection of personally identifiable information ..... 87
18.1.5 Regulation of cryptographic controls ..... 87
18.2 Information Security Reviews ..... 88
18.2.1 Independent review of information security ..... 88
18.2.2 Compliance with security policies and standards ..... 88
18.2.3 Technical compliance review ..... 88

## Introduction

The goal of these Information Security Procedures is to provide information access to authorized users, protect information against unauthorized modification, and information is accessible when needed, whether that information is stored or transmitted on printed media, on computers, in network services, or on computer storage media.

These Procedures contain both rules and guidelines to aid in the interpretation and implementation of the Information Security Policy.

These controls established, implemented, monitored, reviewed and improved, where necessary, to the specific security and business objectives of the organization are met. This should be done in conjunction with other business management processes

## 5. Information Security Procedure Document

**Objective**

The objective of this document is to organize and implement its information security policy by providing systematic procedures to build and enhance the information security.

### 5.1.1 Policies for Information Security

⇒ This document presents the Information Security procedures of the organization.

⇒ The procedures described in this document apply to all controls mentioned in the Information Security policy document of the organization. These controls are applicable to various teams and departments. Implementation of the applicable controls is the responsibility of the team concerned. The identified support teams and departments will assist in implementing the same controls throughout the organization.

**Ownership**

⇒ The Chief Technology Officer (CTO) (Head – IT) will be owner of this document and will be responsible for its development, maintenance, review, and evaluation.

### 5.1.2 Review and Approval

⇒ CIO is responsible to review, update and approve the changes to this document on annual basis and/or if significant changes occur

**Distribution, Change/Version Control**

⇒ This document to be published and communicated to all employees of IBSL and associated services and relevant external parties.

⇒ Information Security Team shall control the change and version of this document

**Scope**

All employees (permanent/temporary/trainee), consultants, contractors, and third parties who use or support organization's computing services or information resources or information processing facilities.

**Structure of this document**

This document is structured as under

**Objectives:** This describes the objectives for having the particular policy control in place.

**The Procedure**: This section describes the procedure or process or guidelines required to implement the control mentioned in the IS security policy

**References:** This section provides reference to other related policy, procedure, process, guidelines & forms.

## 6. Organization of Information Security

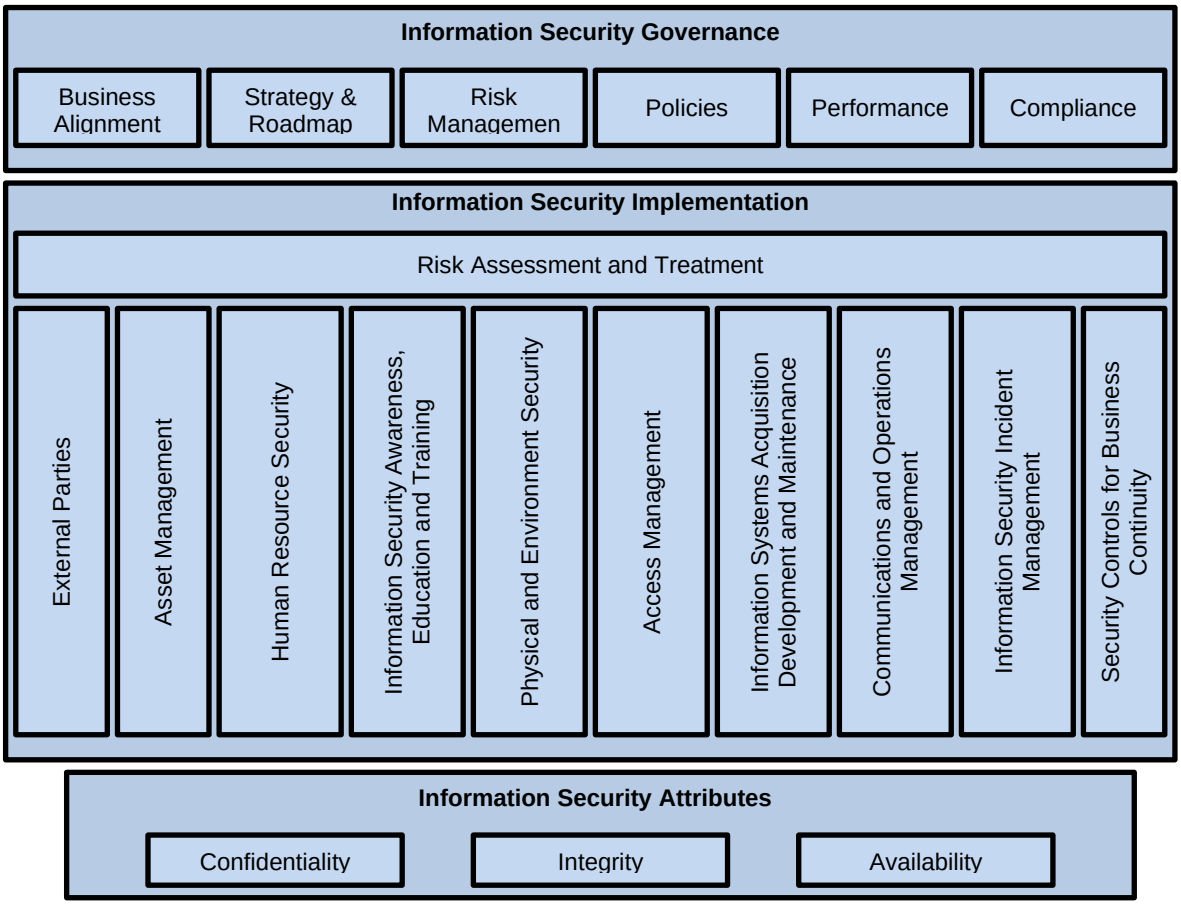
### Objective

Define information security management procedure within the organization.

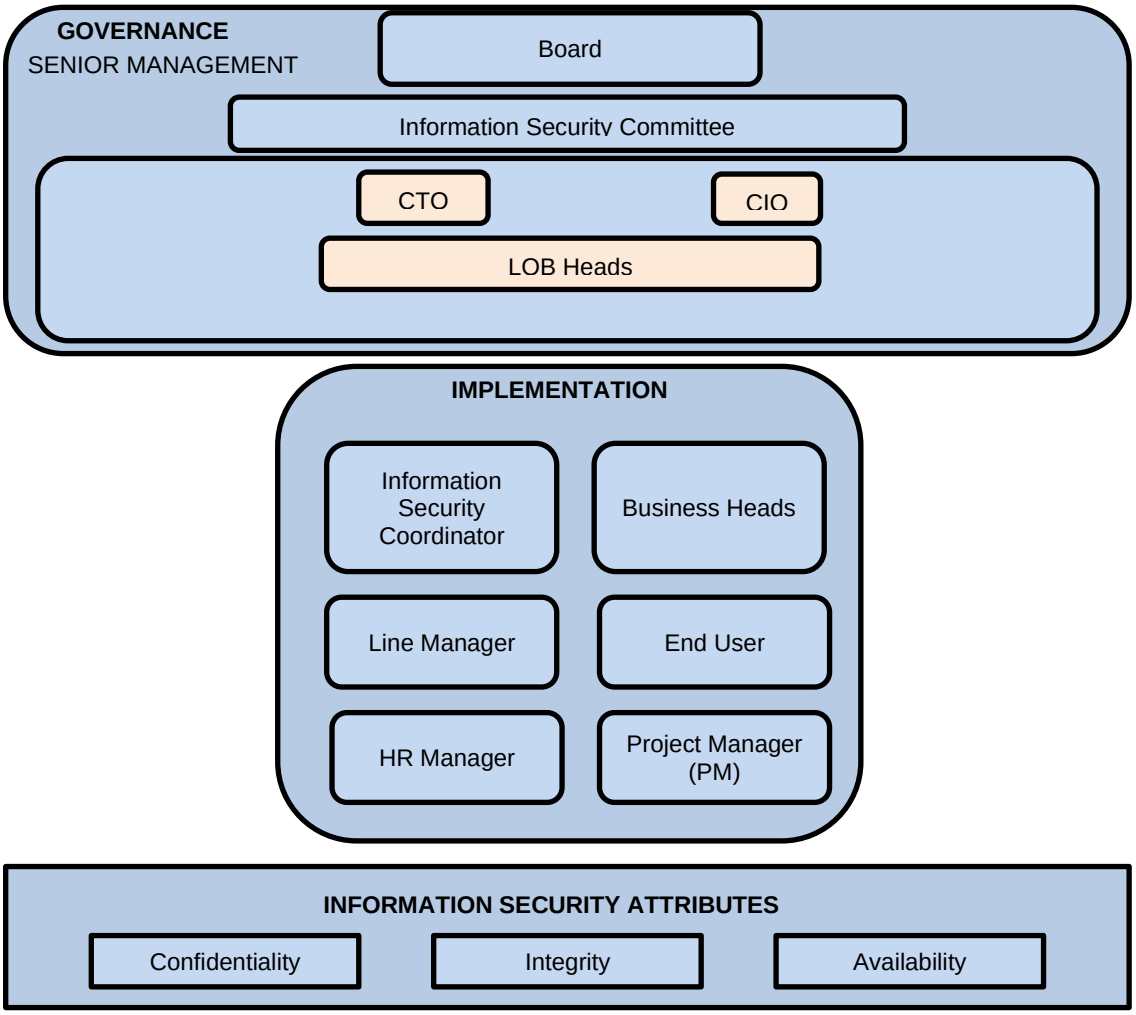
### Procedure

## 6.1 Internal Organization:

Information Security Framework is depicted below:



Organization of Information Security is depicted below:




### 6.1.1 Information Security Roles and Responsibilities

Information Security Governance

## Senior Management

**Roles and Responsibilities**

⇒ Set the high-level direction for how information security should be driven within the IBSL to ensure effectiveness of Information Security governance
⇒ Oversee the working of Information Security Committee and provide directions
⇒ Ratify IBSL's Information Security Policy
⇒ Provide high level direction for integrating information security governance in the overall enterprise governance framework

**Information Security Committee (ISC)**

The committee serves as an effective communication channel for management's aims and directions, and provides on an on-going basis for ensuring alignment of the security program with organizational objectives. ISC is also instrumental in achieving behavior change toward a culture that promotes good security practices and compliance with policies.

**Constitution**
The ISC (Information Security Committee) comprises of the following permanent members.

| |
|---|
| **Mr. P K X Thomas** – CTO (As per IBSL, Head–IT Infra. & Security is CISO, HRM & CISO) |
| **Mr. K. Balachandran** (CFO) |
| **Mr. Shailesh Gupta**- CIO Chief Information Officer (CIO) |
| **Ms. Deepta Rangarajan** (HR Head. / Director Operations) |
| **Mr. Mahesh Tilave** (Application Security Coordinator) |
| **Mr.Sujit Acharya** (Admin In-Charge) |

- Chief Technology Officer (CTO) /Head – Risk Management (HRM) – (As per IBSL nomenclature Head–IT Infra. & Security is CTO and HRM)
- Head – Compliance (HC) - (As per IBSL IT Operations Lead is HC)

CTO will be the convener of the ISC, reporting to CIO.

**Frequency of Information Security Committee meeting**: Semi – Annual

**Roles and Responsibilities**
⇒ At apex level, The Senior Management shall oversee the working of Information Security Committee
⇒ Set the high level direction for how information security should be driven within the IBSL and ratify the Information Security Policy of the IBSL.
⇒ ISC shall oversee the IS security function and shall be responsible for the overall posture of the Information Security of the IBSL.
⇒ Alignment of information security with business strategy to support organizational objectives
⇒ Facilitate in achieving behavior change toward a culture that promotes good security practices
⇒ Monitor compliance with the policies, regulatory and legal requirements of information security
⇒ Providing necessary resources for successful information security
⇒ Management and mitigation of risks and reduction of potential impacts on information resources
⇒ Approve and facilitate the implementation of information security policies, standards
⇒ Approve and monitor major information security projects
⇒ Support the development and implementation of information security management program
⇒ Review the position of security incidents and various information security assessments
⇒ Provide adequate resources and review status of security awareness programs
⇒ Assess new developments or issues relating to information security
⇒ Report to the Senior Management of Directors on information security governance, activities and needs.

| |
|---|
| • **Chief Technology Officer (CTO)** shall be responsible for overall Information Security management of the IBSL. |
| • **Chief Information Officer (CIO)** shall be closely associated with the CTO and Head of Risk Management to assist in defining the Information Security Policy & Framework, selection of the technology platform for information security, guiding the strategy and implementation of the information security plan and shall provide sponsorship to drive the information security program across Information Technology throughout the organization. |
| • **Line Manager / Business Heads / Security Coordinator / Project Manager (PM)** |

| |
|---|
| shall be responsible to alignment of information security program to their business needs and shall provide sponsorship by driving the information security program to the teams under their management and mandate compliance to Information Security Policy. |

## Roles and Responsibilities of Special Interest Groups

**End Users / Business User**
End User's an employee, contractor, consultant, vendor etc. of the IBSL who use information systems resources as part of their job

⇒ Responsible and accountable for the activities performed using user ids assigned
⇒ Maintain confidentiality of log-in password(s) and ensured that they are not shared
⇒ Ensure security of information entrusted to their care
⇒ Use IBSL business assets for the approved purposes only
⇒ Understand and adhere to all information security policies, procedures, standards and guidelines
⇒ Promptly report security incidents, suspicious activities/events, policy violation to management/security administration.

**HR Head**
HR Manager is the manager or supervisor of employee who belongs to HR functions and is responsible for all HR related activities of the organization

⇒ Inform ITSS Team of the on-boarding of any employees/contractors.
⇒ Inform access rights administration / security administration of the terminations.
⇒ Inform access rights administration / security administration of the transfers.
⇒ employees are aware of relevant security policies, procedures
⇒ Establish accountability for security through clear job descriptions, employment agreements
⇒ Initiate necessary disciplinary action for the violations

**Information Custodian / IT Infra Team / Security Coordinator**
Information Custodian is an information technology official (IT Infra Head), is the delegate of the Business Information/ Application Owner who is responsible for development and maintenance of the application/infrastructure within their environments for the respective business function

⇒ Ensure security of Information assets in accordance with the business needs aligned to information security policy and procedures
⇒ Information/asset classification/de-classification and periodically reviewing the classification to ensure it still meets business needs
⇒ Risk assessment and management in accordance with the policy.
⇒ Ensuring that the Change Management process is followed for any changes in application
⇒ Take appropriate actions on security violations when notified by the security administration
⇒ When necessary, restoring/recovering lost or corrupted information from backup media to return the application to production status

## 6.1.2 Segregation of Duties

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Segregate duties and areas of responsibility to reduce | CIO |

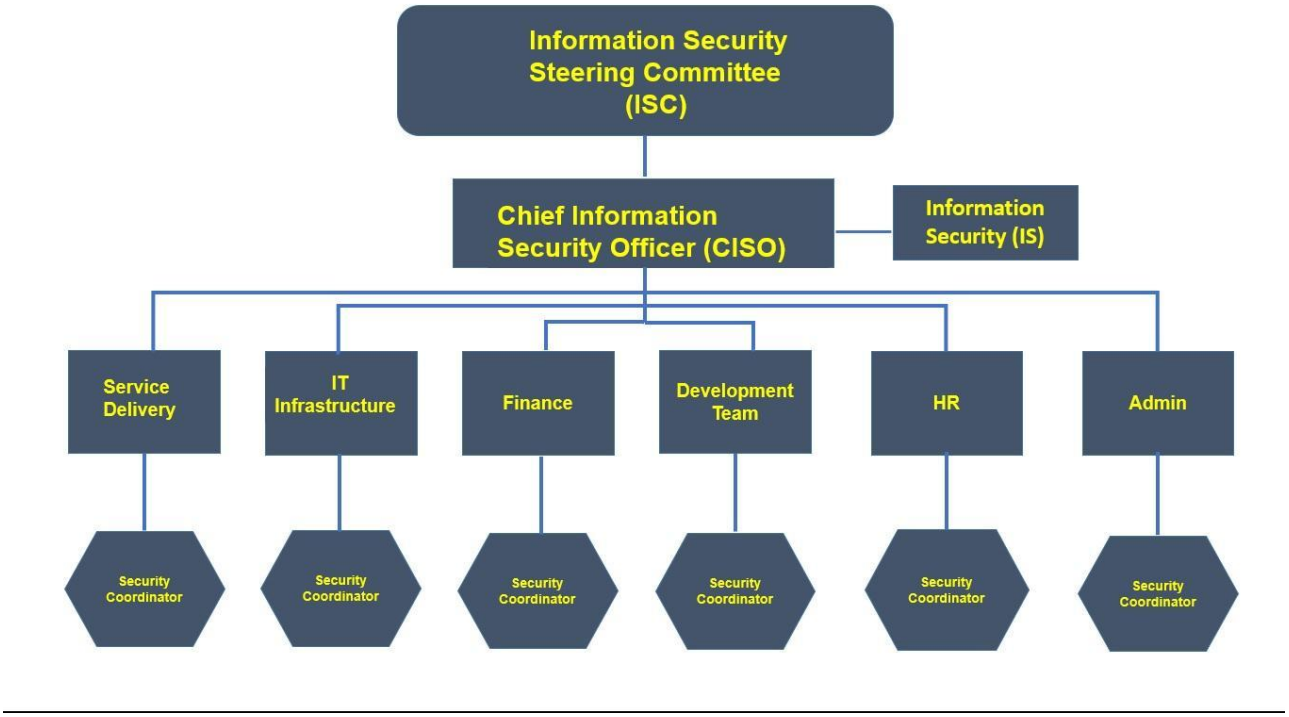
| | | |
|---|---|---|
| | opportunities for conflicting duties.<br><br>Please refer clause 6.1.1. Information Security Roles and Responsibilities | |

### 6.1.3 Contact with Authorities

The Support functions shall maintain contacts with the relevant regulatory authorities, utilities, emergency services and other authorities as required. Following is the list of authorised agencies (but not limited to) to be contacted;

- CERT-IN for Information Security related incidents.
- Local Law and Order and/or Fire department for Physical Security related incidents.
- Zonal EPFO for Employee Dues
- GSP for tax filing
- Also, an internal Emergency Response Team is formed and trained to handle emergency situations in the organisation. Contact details of ERT are made available to employees.

**Security Organization Chart**




### 6.1.4 Contact with Special Interest Groups (Support from End users)

**Following are the special interest groups involved in ISMS implementation. Their roles and responsibilities are defined in above Section**

**End Users / Business User**

End User's an employee, contractor, consultant, vendor etc. of the IBSL who use information systems resources as part of their job

**HR Head**
HR Manager is the manager or supervisor of employee who belongs to HR functions and is responsible for all HR related activities of the organization

**Information Custodian / IT Infra Team / Security Coordinator**
Information Custodian is an information technology official (IT Infra Head), is the delegate of the Business Information/ Application Owner who is responsible for development and maintenance of the application/infrastructure within their environments for the respective business function

### 6.1.5 Information Security in Project Management

All projects basically need resources, activities to develop, and established time objectives. Information security can be integrated into project management activities in several ways:

⇒ Include information security objectives in project objectives.
⇒ Perform a risk assessment in an early stage of the project.
⇒ Carry out treatment of the identified risks and implement security measures

⇒ Make the information security policy an indispensable part of all stages of the project

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Define & establish information security in projects as & when required for small & big types of internal/external projects. | CTO / PM |

## 6.2 Mobile devices and Teleworking

### 6.2.1 & 6.2.2 Mobile Computing & Teleworking

**Mobile Computing &Telecommuting Security Measures**

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Configure and enforce that all remote connections and communications to the IBSLnetwork have the following controls:<br>● Official Mail Id's has been configured on the requested user's mobile devices<br>● Remote connections for teleworking purposes should be approved by the line manager | IT Infra. Team |

### 6.2.3 Information Security Measures for remote working during Pandemic period

| Sr.No. | Activity | Responsible |
|---|---|---|
| 1 | VPN technology is implemented to support remote working | ITSS |
| 2 | Antivirus service is implemented on all personal desktops / laptops to protect from viruses / malware / persistent threats etc. | ITSS |
| 3 | Vulnerability and malware scanning shall be scheduled daily. Windows patches are pushed into the end users' systems through FortiClient VPN tool. | ITSS |
| 4 | Remote meeting tools i.e.Google Meet shall be implemented to support Video conferencing, Communication between employees and clients | ITSS |
| 5 | Information Security Awareness pertaining to Information security while work from home / remote is shared with all employees. | ITSS |

**User Enforcement**

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Sensitive information is not stored/ processed/ transmitted outside IBSL network and conduct activity in accordance with the IBSL Information Security Policy and does not damage/harm the Organization (IBSL) in anyway. | Business User |
| 2 | Do not work on any IBSL information where it can be viewed by unauthorized individuals, either in public places or in areas where un-trusted networks and systems are used. | Business User |
| 3 | Conduct awareness sessions to educate the user regarding following best practices of mobile device usage:<br>● Adequate physical security and access controls mobile computing and telecommuting<br>● The risks of using mobile computing and telecommuting<br>● Securely connecting mobile computing and telecommuting to network and using outside the organization. | IT Infra. Team. |

**Work From Home Security Measures**

For remote working, IBSL has provided VPN connectivity to all employees who are using corporate Desktops / Laptops remotely.

To strengthen the security protection on such desktops / laptops following measures have been implemented:

- FortiClient VPN is deployed in all corporate laptops/desktops to connect to IBSL's network remotely.
- Deployed Sophos Antivirus on all corporate desktops/laptops to protect from viruses/malware/persistent threats etc.
- Real time monitoring is enabled in Sophos Antivirus and necessary alerts are generated for all systems.
- Password policy and account lockout policy is enabled on all windows systems as per section 9.2 & 9.3 of this document.

**Common Do's and Don'ts of Work From Home**

- Don't share photos of your workstation at home on social media
- Do protect the details about work-from-home from social media
- Don't share your office laptop with family members or friends or close relatives
- Do use VPN connectivity to connect to office environment for all official work
- Do save your official documents on the shared folders provided to you post connecting to the VPN
- Do not open / save office documents locally on your desktop / laptop (BYOD) without prior permission
- Do ensure safe internet usage, avoid visiting unknown sites / malicious websites or clicking on suspicious links while working on office work
- Do keep office passwords different from personal passwords

- Do ensure to lock the screen while you go away from the desktop / laptop
- Do ensure physical security of your desktop / laptop, Keep it in lock and key when not in use. Protect it from thefts
- Do not use publicly available free WiFi to connect VPN
- Do change home WiFi password at regular intervals
- Do ensure that you are vigilant about Email Phishing and Ransomware attacks
- Do not respond to mail received from unknown sender
- Do not click on any links received from unsolicited email
- Do not share your confidential information on Social Media or links received from unknown senders
- Do ensure OS and Anti-virus patches are deployed on regular basis and they are up to date

# 7.0 Human Resource Security Procedure

## 7.1 Prior to employment

**Objective**
Objective of this procedure to define & maintain steps to reduce the risk of human error, theft, fraud or misuse of facilities.

**Procedure**

### 7.1.1 Screening

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Prepare job description based on the profile required. Define Security roles and responsibilities of employees, contractors and third party users in accordance with the IBSL's information security policy. | HR |
| 2 | Communicate security roles and responsibility to job candidates and third party employees during the pre-employment process. | HR |
| 3 | Profiles matching the job descriptions must be short-listed and interviewed. References must be obtained in candidate information form<br><br>Interview details shall be captured in an excel sheet which shall be maintained at offices | HR |
| 4 | Conduct verification and reference check before recruiting a person as permanent employee, These includes references, academic and curriculum proofs, identity checks etc.<br><br>Candidates shall be screened, interviewed, shortlisted and selected, screening is based on business & project requirements.<br><br>Xerox copies of the documents shall be verified against the originals.<br><br>Xerox copies of identity and address proofs and educational certificates shall be treated as personal and sensitive information and shall be kept under lock and key preferably in a locked cupboard or cabinet. | HR |

### 7.1.2 Terms and conditions of employment

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Enforce that all the employees sign confidentiality and non-disclosure agreements (NDA) at the point of joining | HR |
| 2 | Third party user, casual staff or consultants having access to information processing facilities sign a confidentiality agreement | Admin |
| 3 | Store signed confidentiality agreements | HR |
| 4 | Upon initiation of contract and all employees shall sign a letter of engagement on initiation of employment. | HR |

## 7.2 During employment

**Objective**
To users are aware of information security threats and concerns and are equipped to support the organizational security policy in course of their normal work.

**Procedure**

### 7.2.1 Management responsibilities

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Employee's responsibilities for information security and disciplinary actions against violation are mentioned in the terms and conditions of the employment. | HR |
| 2 | Ensure employee contract agreement addresses the information security requirements and incorporates all the required clauses and it complies with all applicable laws and regulations using legally enforceable terms | HR |
| 3 | Do not give access to new and inexperienced staffs to critical and sensitive information without authorization. The employees are granted access to information/ information system as per the Access Management Procedure | Management |
| 4 | Security roles and responsibilities for employee are defined and documented<br><br>Please refer Responsibilities for End Users / Business User in 6.1.1. | IT Infra Team |
| 5 | Comply with the Information Security Policy. When in doubt, seek guidance and clarifications from their line management or Security coordinator for policy interpretations. | End User |

### 7.2.2 Information security awareness, education and training

⇒ The goals of a successful information security awareness program is to ensure, that all employees of IBSL are aware of the policies and procedures set in place to protect and safeguard company confidential data.
⇒ Training programs will be conducted on bi-annual basis.
⇒ A program shall be considered successful if it meets the following conditions:
⇒ Individual employee, staff are aware of risks to the confidentiality, integrity, and availability of data, and know how to protect data.

⇒ When there are valid reasons for suspecting theft, damage, or misuse of data, the individual knows what to do (who to contact and how).

**Identify Trainers**

⇒ Primary responsibility of the Information security awareness program will be with HR Team.

⇒ CTO shall identify appropriate trainers to conduct information security awareness training program for their organization.

⇒ Security Coordinator Team shall be trained on various technologies deployed in the organization, to furnish them with the knowledge required for conducting the information security awareness training program for the organization.

**Prepare the Training Material**

⇒ Following are the bare minimum topics that shall be covered in the training:
- Password Construction
- Internet Usage
- Telephone Fraud
- Physical Security
- E-mail Usage

⇒ Information Security awareness training:
- To be included as a part of employee induction program
- Annual information security awareness refreshers program to be conducted for all employees

**Conduct the Training**

⇒ Ensure all participants are informed about schedule, to ensure participation.

⇒ Any last moment changes shall be avoided and non - participation shall be approved by reporting manager/ HOD.

⇒ HR Team to track and ensure all employees have undergone the training annually.

**Evaluate the Program**

⇒ All employees shall be requested to fill a feedback form for the training

⇒ Attendance sheet and the feedback form collected for the training shall be maintained by HR Team

⇒ Measure the success of the awareness program by reviewing the feedback forms to identify the strengths and weakness of the program.

### 7.2.3 Disciplinary Process

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Code of conduct has been defined by HR which denotes the disciplinary actions to be taken for non-conformance | HR |

## 7.3 Termination and change of employment

### 7.3.1 Termination responsibilities

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Forward the employee resignation letter or termination/ retirement intimation to the HR | Line Manager / Employee |
| 2 | Get all the required clearances and submit it to HR | Employee |
| 3 | Enforce that ex-employee also cannot disclose any information to public. | HR |
| 4 | Update employee master file | HR |
| 5 | Review return of assets in possession upon termination of the employment, contract or agreement | HR |

## 8 Asset Management Procedure

**Objective**
Primarily there are two categories for assets. One is end user assets and other one is Server related Assets.

**Procedure**

### 8.1 Responsibility for Assets

#### 8.1.1 Inventory of assets

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | IT Infra. Team will an inventory is maintained of all assets (Information Systems and Processes) under their control. The inventory will specifically identify at minimum the following :<br><br>1) Business Application Department<br><br>2) Type of Asset<br><br>3) Serial Number of Asset<br><br>4) Asset Ownership<br><br>5) Location of Asset<br><br>6) Status of Asset (Scrapped/In-Use)<br><br>(Refer: Asset Register) | IT Infra. Team. |

| | | |
|---|---|---|
| 2 | Identify the various assets used in respective area. Consider the following asset types:<br><br>o Information Assets:<br>Data stored in databases and data stored in electronic files (word, excel, text, xml etc.), contracts and agreements, standard operating procedures, system documentation, Physical assets.<br>o Software Assets:<br>Business Application software, system software (OS, Databases, web server, application server etc.), development tools and utilities<br>o Services:<br>Computing and communication services, general utilities (e.g. AWS, Azure, email, Internet link, lighting, power, air-conditioning) | IT Infra. Team , PM |

| | | |
|---|---|---|
| | ○ People:<br>People and their titles, People holding sensitive information or access to sensitive information should be identified. These people should be made aware of the controls that are needed for security of such information. | |
| 3 | Ensure asset register is updated as and when there is change.<br><br>On annual basis review and obtain approval from CTO on asset register. | IT Infra. Team. |

### 8.1.2 Ownership of Assets

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | All information / data and assets associated with the information processing facilities shall be owned by the designated person of the IBSL as a “Business Owner” who is responsible for controlling, the production, development, maintenance, use and security of the assets | Business Owner |

### 8.1.3 Acceptable use of assets

| Sr. No. | Activity | Responsible |
|---|---|---|
| General Use and Ownership | | |
| 1 | Users should familiarize themselves with the IBSL's Information Security Policies and Procedures.<br><br>Users should any sensitive or vulnerable information is stored in a safe place.<br><br>Preventing the misuse of the assigned Access Card/ Visitor Badge is the responsibility of the card/ badge holder.<br><br>Users should always remain alert and notify immediately in case they notice or suspect any violation of IBSL's Information Security Policies to the Information Security team<br><br>Copyright and licensing agreements shall not be violated.<br><br>Use of any un-authorized software is strictly prohibited<br><br>Any attempt to circumvent IBSL’s security policy procedures shall be viewed as a breach of code of conduct.<br><br>All employees, contractors, consultants, vendors and third party users shall acknowledge understanding and acceptance of IBSL’s information security policy by signing the suitable undertaking and/or agreement.<br><br>All contractors, consultants, vendors and third parties shall obtain | End Users |

| | | |
|---|---|---|
| | suitable undertaking and/or agreement signed by their respective employees who are using or accessing IBSL's information systems.<br><br>Use of unauthorized removable media such as floppy, USB, CD etc. should be prohibited | |
| Email Usage | | |
| | E-mail shall be used for business purposes only. Use of e-mail for personal use is discouraged.<br>User shall only use their official email id for business communication<br><br>Forwarding of the chain emails is strictly prohibited.<br><br>Information classified as 'Confidential' should not be emailed to anyone unless approval is sought from owner of the information | End Users |
| Internet Usage | | |
| | All users should use the Internet in accordance with the policy and for the intended business purpose only.<br><br>All users should browse the Internet only through official channel and should not use any other means to override the implemented access restrictions on Internet usage<br><br>Internet access provided by the IBSL shall not be used to engage in any activity that knowingly contravenes the law (IT Act 2000, Copyright Act etc.).<br><br>Downloading programs and executable files from the Internet is strictly prohibited. | End Users |
| Information Publishing | | |
| | Release of information shall be in accordance with IBSL's policy and shall follow authorization mechanism<br><br>Publishing the IBSL's proprietary information or brand on internet through blogs, news groups, collaboration or social networking sites is prohibited and shall be done only by authorized department i.e. Marketing and Corporate Communication. | End Users |
| Use of Mobile / Portable Device | | |
| | Users should use the mobile devices such as laptops, handheld devices etc. provided by the IBSL for business purposes.<br><br>Users should ensure the antivirus and spyware protection is enabled and updated to latest one while connecting to IBSL's network from outside network. | End Users |
| Malware / Virus Protection | | |
| | Users shall be responsible to the anti-malware / virus solution is latest | End Users |

| | | |
|---|---|---|
| | and up to date on their desktops and laptops; and in case of any issue contact IT support team for remediation.<br><br>Users shall be responsible for scanning the files obtained within IBSL or from external sources using removable storage | |

### 8.1.4 Return of Assets

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Return IBSL's assets in possession upon termination of the employment, contract or agreement.<br><br>Respective department/owner should sign the handover form. | Employees/ contractors/ third party users |

## 8.2 Information classification

### 8.2.1 Classification of information

| Terms and Reference |
| --- |
| Formal information labeling is utilized regardless of the media on which information is stored, the systems that process it, or the methods by which it is transmitted.<br><br>The different classes of assets and information(electronic/documentation) are labeled as outlined below:<br><br>**High or Confidential:**<br>Assets or Information which, if mishandled, may cause damage to the organization. It is sensitive to both internal as well as external exposure.<br><br>**Moderate or Medium:**<br>Assets or Information, which is sensitive to external exposure only and any unauthorized disclosure would cause embarrassment or difficulty to the organization or whose loss would cause moderate, but recoverable damage to the organization.<br><br>**Low or Public:**<br>Assets or Information which has been expressly approved for release to the public. It applies to information for which unauthorized public disclosure would have no significant negative impact or consequences for the organization.<br><br>Classification applicable for physical assets:<br><br>**1 -** Low value<br><br>**2 -** Moderate value<br><br>**3 -** High value<br><br>**4 -** Critical value<br><br>**5 -** Mission Critical value<br><br>Classification Methodology:<br><br>• Classification exercise to be carried out for the identify assets as per defined asset types.<br><br>Review Frequency:<br><br>• CTO will review the IT Asset register Semi Annually. |

**Information and Asset Classification Procedure**

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Identify asset and conduct the classification exercise as per below defined classification guidelines and methodology<br><br>**1** – Low. Can be addressed as part of routine operations<br><br>**2** - Moderate impact. Effectiveness of services would be threatened, but can be dealt with.<br><br>**3** - High impact. May significantly affect business services and/or result in some financial loss<br><br>**4** - Critical impact. May result in disastrous consequences and/or lead to significant financial loss<br><br>**5** – Mission Critical impact. May lead complete standstill of business operations. Would take considerable time to fully recover. | IT Infra. Team |

### 8.2.2 Labeling of information

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Physical assets are labeled using appropriate asset tag & classification is maintained in asset register. | IT Infra Team |

### 8.2.3 Handling of assets

| Sr. No. | Activity | Responsible |
|---|---|---|
| Following handling procedures should be implemented | | |
| 1 | Maintain all Information Assets in an Information Asset Register. | IT Infra. |
| 2 | All information assets are accounted for and have a designated owner assigned named as “Business Information Owner”. | IT Infra. |
| 3 | The classification of information resources is done based on Asset classification. | IT Infra |
| 4 | Review the information at least annually to determine if any change in the status of its classification. | CTO |

## 8.3 Media handling

### 8.3.1 Management of removable media

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Only with the prior authority approval removable media is permitted for data transfer purposes. | Head IT |
| 2 | Lock away sensitive or critical business information when not required. | End User |

### 8.3.2 Disposal of media

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | ● No removable media is being used as and removable medias are not allowed in IRIS<br>● Users intimate about the Information Assets that are not usable further with the details of assets to the infrastructure group | End User |
| 2 | ● Assets are inspected and the authorization for disposal are obtained<br>● If the asset contains any data/ license, the data have to be uninstalled before disposal<br>● For assets on lease, upon termination of lease agreements; the assets are reviewed by IT Infrastructure group and assets which are likely to have data/license are returned only after ensuring that data/license have been removed.<br>● Upon transferring the asset, the details of non-returnable gate pass is entered in the register | CTO |
| 3 | Destruction of Magnetic Data and Media:<br>● Prior to disposal, all storage media, equipment, or systems containing fixed hard disks are checked to ensure that all sensitive data and licensed software has been overwritten or removed<br>● A third-party media destruction company is used if that company can provide a green certificate of destruction | CTO |
| 4 | Hardware scraping of ISBL assets is outsourced to a vendor. An e-waste certificate is provided by the vendor on completion of the services. | CTO |

| | | |
|---|---|---|
| 5 | Destruction of Paper Media:<br>● Paper documents that contain sensitive information is shredded or incinerated in all branch locations. | CTO |
| 6 | Disposal of damaged storage devices:<br>● Ensure that damaged storage devices containing sensitive data are evaluated and decide whether the damaged items are destroyed, repaired or discarded<br>● Ensure that due care is taken that sensitive data or licenses are not left with the device while discarding or sending the repair outside | CTO |

### 8.3.3 Physical media transfer

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | There is no media transfer activity performed. | IT Head |

# 9 Access Control Procedure

**Objective**
The objective is to control access to information and business processes based on business and security requirements. It aims to protect and detect unauthorized access to information systems.

**Procedure**

## 9.1 Business Requirement for Access Controls

### 9.1.1 Access control policy

**Access Control Rules**
Access control to information assets will be given to various users and group of users based on following rules, which will always be enforced:

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Access control will be on “need to know” and “need to use” basis. This implies that users will access only the information which is required to be known or is being used for appropriate functioning of their activities. | IT Infra Team |
| 2 | Access rights will be given only after defined administrative approval | Respective Owner / Supervisor/Line Manager |
| 3 | Access to critical information systems such as modules of IRIS System will be through distinct Id and password protection | Respective Owner / Supervisor/Line Manager |
| 4 | Users will be given appropriate rights of read, write, modify for providing differential control on information | Respective Owner / Supervisor/Line Manager |

### 9.1.2 Access to network and network services

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Segregate network into separate logical network segments to create security perimeter by considering the following:<br>● Identifying all access points to the network such as internet | IT Infra Team. |

| | | |
|---|---|---|
| | and intranet including remote access.<br>● Implement Firewall to control access and traffic flow to block unauthorized access<br>Prepare detailed network architecture document and obtain approval from CTO | |
| 2 | On quarterly basis review and approve the network architecture document. | IT Head/ CTO |

**Remote access and user authentication for external connection**

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Provisioning and Registration for Network/Remote/Emergency Access/Wireless Access Users. | IT Infra Team |
| 2 | All users seeking to gain access to the IBSL's IT facilities via public or other external networks should connect using virtual private network (VPN)<br>Access authorization for users and applications published over VPN<br>Remote access shall be allowed to systems and applications only after following the authorization mechanism | IT Infra Team |
| 3 | All remote communication happens through a secure and encrypted channel | IT Infra Team |
| 4 | Communication traffic is forced through a firewall so that the firewall can detect and mitigate any malicious content or behavior. | IT Infra Team |
| 5 | Only secure access protocols should be allowed on network devices. | IT Head /CTO |

## 9.2 User Access Management

### 9.2.1 User registration and deregistration process

**Registration Process**

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Email access request from HR/ Department Head will be forwarded to IT team to provide the access. Indicate the necessary information/data access required for the user to perform his/her day-to-day activities.<br><br>For non-IBSL employees, the process remains the same. | HR / Business Owner |
| 2 | Approval or rejection of the form based on need-to-know and need-to-use basis and if the provision of access does not violate any Segregation of duties matrix. If form is rejected inform to the line Manager | IT Head |
| 3 | Create a record for all ID creation/modification request and send it to the administrator for action. | IT Infra Team / HR |
| 4 | Create/modify user in the system. | IT Infra Team |
| 5 | Informs New ID details to requestor and his reporting manager and HR about the completion of the task. | IT Infra Team |

**De-registration process**

| Sr No | Activity | Responsible |
|---|---|---|
| 1 | Notify the HR for access revocation. | Line Manager |
| 2 | Forward the details of the user to the IT Infra Team | HR |
| 3 | Revoke, if any, privilege/ Internet/Network/Remote/Emergency Access/Removable Media/Wireless access granted to the user and disable user account. | IT Infra Team |

| | | |
|---|---|---|
| 4 | Return all resources to the IT Team/Admin | End User |
| 5 | Backup all user related data and lock user account on exit date. | IT Infra Team |

### 9.2.2 Use access provisioning

**User Provisioning and Registration for Network/Remote/Emergency**

**Access/Wireless Access Users**

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Provisioning access request from Line Manager will be forwarded to IT team to provide the access. Indicate the necessary information/data access required for the user to perform his/her day-to-day activities.<br><br>For non-IBSL employees, the process remains the same. | Line Manager |
| 2 | Approval or rejection of the form based on need-to-know and need-to-use basis and if the provision of access does not violate any Segregation of duties controls. If form is rejected inform to the line Manager | IT Head |
| 3 | Provide/modify access for Network/Remote/Emergency Access/Wireless Access Users | IT Infra Team |
| 4 | Inform change details to requestor and his reporting manager about the completion of the task. | IT Infra Team |

**User Provisioning and Registration for Removable Media Access**

| Sr. No | Activity | Responsible |
|---|---|---|
| 1 | Raise a request with business justification at IT Infra Team to seek necessary approval to allow removable media access | Requestor/ Line Manager |
| 2 | Validate and approve/reject the request. Inform the requestor. List of considerations for approving access and summary of requests | Business Owner/CTO |

| | | |
|---|---|---|
| | and disposal considerations. | |
| 3 | Provide access on Symantec end point application | IT Infra Team |
| 4 | Inform details regarding the access to requestor and his reporting manager and IT Head about the completion of the task. | IT Infra Team |

### 9.2.3 Management of privileged access rights

| Sr. No | Activity | Responsible |
|---|---|---|
| 1 | Raise a request with business justification at IT Infra Team to seek necessary approval to allow Privileged access. | Requestor/ Line Manager |
| 2 | Validate and approve/reject the request. Inform the requestor. List of considerations for approving access. | IT Head |
| 3 | Provide access as requested | IT Infra Team |
| 4 | Inform details regarding the access to requestor and his reporting manager and IT Head about completion of the task. | IT Infra Team |

### 9.2.4 Management of secret authentication information of users

| Sr. No | Activity | Responsible |
|---|---|---|
| 1 | Only administrator will be able to make changes in the system configurations.<br><br>Provide administrative rights on the basis of business need & approvals from line manager/business owner. | IT Infra Team / IT Head / Line Manager |

### 9.2.5 Review of user access rights

| Sr. No | Activity | Responsible |
|---|---|---|

| Employment Re-validation on quarterly Basis | | |
|---|---|---|
| I | Perform employment re-validation of on-roll/outsourced/contracted employees to review active user-ids against the employment status on a quarterly basis covering following types of user-ids<br><br>End user-ids<br>Privilege user-ids<br>System accounts/Generic privileged user-ids<br>Generic user-ids | IT Head and Business owner |
| 1 | Get the list of separated and resigned on-roll/outsourced/contracted employees, from HR and/or respective business functions. | IT Infra Team |
| 2 | Generate the list of various active user-ids and reconcile against the list of separated and resigned on-roll/outsourced/contracted employees | IT Infra Team |
| 3 | Report any gap noted in reconciliation to respective IT Infra Head/business operations owner/business application owner | IT Infra Team |
| 4 | Review reconciliation gap report and accord approval to delete/disable the user-ids that are not assigned to active on-roll/outsourced/contracted employees | IT Head/Business owner/ HR |
| 5 | Delete/disable the user-ids as per the approval granted | IT Infra Team |

### 9.2.6 Removal or adjustment of user access rights

**Approval process**

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Raise a request with business justification to IT team to seek necessary approval to allow access which is not allowed as per policy | Line Manager / Business Owner |
| 2 | Approve/reject the request | IT Head |
| 3 | Grant access to user as per request | IT Infra Team |

**Renewal process**

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Raise a revalidation request at IT team | HR / Line Manager |
| 2 | Approve/reject the request | Business Owner |
| 3 | Renewal access as requested | IT Infra Team |

**System accounts and generic accounts**

| Sr. No. | Activity | Responsible |
|---|---|---|
| **System Accounts and Generic Privileged Accounts** | | |
| 1 | Wherever possible system/generic privileged user-id or default system account should be disabled | IT Infra Team / IT Head |
| 2 | Document the business and/or operational need of using system/generic privileged user-id and user & owner | IT Infra Team / IT Head |
| 3 | Use of system/generic privileged user-id to be validated and approved | IT Infra Team |
| 4 | Review system/generic privileged user-id on a quarterly basis as per the user access review procedure | IT Head |

## 9.3 User Responsibilities

### 9.3.1 Use of secret authentication control

**Password Use**

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | All activities performed with a particular user ID shall be monitored and the user shall be held accountable for any activity carried out under his/her ID.<br><br>Users should not share their password to another user for any purpose<br><br>Users should understand and select the password as per the password policy.<br><br>Users should change the passwords at regular intervals or at the time of suspected password compromise.<br><br>Select strong / quality passwords as per above password policy | End-Users/System Administrators |

**Password policy**

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | ● Password length shall be minimum 12 characters; password phrase shall be used where possible.<br><br>● Password shall be combination of alphanumeric characters, special characters shall be used where possible<br><br>● Blank password shall not be permitted<br><br>● Default passwords shall be changed<br><br>● Last 3 passwords shall not be used<br><br>● User ids shall be locked after 3 repeated unsuccessful attempts<br><br>● Password Age: Passwords shall be changed every 60 days at a minimum<br><br>● User passwords shall not be stored in automated login process.<br><br>● Passwords shall never be stored or transmitted in clear text.<br><br>● Passwords shall not be displayed in plain text on the screen while being entered, must be masked. | End-Users/System Administrators |

| | | |
|---|---|---|
| | ● A password shall be changed if it is compromised or disclosure is suspected.<br><br>● Users must be forced by the system to change the initial password on first successful log-on | |

## 9.4 System and application access control

### 9.4.1 Information access restriction

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Access to information and application system functions by users and support personnel are restricted in accordance with the defined access control policy. | IT Infra Head |

### 9.4.2 Secure logon procedures

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | All activities performed with a particular user ID shall be monitored and the user shall be held accountable for any activity carried out under his/her ID.<br><br>User should keep their passwords confidential<br><br>Users should change the temporary and/or default passwords provided at the first log-on.<br><br>Users should not include passwords in any automated log-on process, e.g. stored in a macro or function key. | End Users |

### 9.4.3 Password management system

| Sr. No. | Activity | Responsible |
|---|---|---|
| New Password Allocation | | |
| 1 | Allocate user-id and password to users while creation of access | IT Infra. Team |
| 2 | Provide temporary password to user and send confirmation mail after password allocation | IT Infra Team |
| 3 | Change the temporary password on first logon to the system | End User |

| Password Reset | | |
|---|---|---|
| 1 | Configure user-id to suspend the system after three (3) unsuccessful attempts to enter a password | IT Infra team |
| 2 | Raise a service request when locked out of an application as a result of surpassing the set threshold for login | Line Manager |

**Privilege Password Storage**

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Passwords to privileged access to critical systems are sealed in an envelope. | IT Head |
| 2 | When privileged users change this password, the same is updated in the sealed envelope document | IT Head |

### 9.4.4 Use of privileged utility programs

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Privileged utilities are provided on request as predefined by IT Head & Business Owner | CTO |

### 9.4.5 Access control to program source code

| Sr. No | Activity | Responsible |
|---|---|---|
| 1 | Do not maintain program source libraries in operational systems and is issued, controlled and updated by authorized personnel. | Business Owner |
| 2 | Provide restricted access to program source libraries and audit log is maintained for all accesses. | Application administrator |
| 3 | Do not hold the program source code under development. | Application administrator |

| | | |
|---|---|---|
| 4 | Old versions of source programs are archived with details of operational date and time, supporting software, job control, data definitions and procedures. | Program librarian |

# 10 Cryptography

## 10.1 Cryptographic Controls

### 10.1.1 Policy on the use of cryptographic controls

| Sr. No | Description | Responsible |
|---|---|---|
| 1 | Assess, document and deploy cryptographic controls and solutions to ensure security of information in accordance with degree of confidentiality and integrity required for information as per business, regulatory and legal requirements. | Developers |
| 2 | Obtain approval from CTO for the cryptographic controls proposed and used | Developers |
| 3 | The AES 256 SSL certificate is used from reputed international certificate authority to protect the websites for:<br>● All online channels published over Internet<br>● All websites classified as critical and above which is processing any information published over Internet except informative websites i.e. corporate website<br>● Use Extended Validation-SSL certificates for customer facing online delivery channels | Business Application Owners / IT Heads |
| 4 | Where appropriate, transaction security ensured through Key encryption and verification. | Business Application Owners / IT Heads |
| 5 | Ensure network communication used for any interconnections with external parties over external networks and public network for the purpose of file transfer, data transfer, interactive access, application access is encrypted by using:<br>● IP-Sec-AES/3-DES/DES for data encryption | Developers |
| 6 | Ensure secure transmission of the confidential data/files being exchanged with external parties over external networks or public network or removable storage media by using:<br>● Secure FTP or SFTP or FTPS for FTP Server used for sharing<br>● 128-bit SSL certificate for Website used for sharing | Business Application Owners / IT Heads |
| 7 | Ensure use of digital signature certificate (DSC) for the purpose of authentication, signing and encryption of electronic documents, transactions, and data where non-repudiation of a sender i.e. where there is need to verify who has signed electronically and integrity of data in transit i.e. to check whether the contents of the signed data is not changed in transit; is required in accordance with the applicable law. | Developers |

| | | |
|---|---|---|
| 8 | Ensure use of digital signature certificate (DSC) issued by licensed Certifying Authority (CA) under Controller of Certifying Authorities (CCA) of Government of India for the purpose of digital signature where it is required in accordance with the applicable law under Section 24 of the Indian IT-Act 2000.<br><br>Assess & use type of DSC either Class 2 or Class 3 in accordance with business need & law<br><br>Maintain record of DSCs including validity, users etc. and review on yearly basis | Developers |
| 9 | The passwords stored by the information systems are encrypted | Business Application Owners / IT Heads |
| 7 | Ensure AES encryption with at least WPA2 protection between wireless client and WAP for wireless communication. | IT Infrastructure Operations Head |
| 9 | Review encryption algorithm and standards on a yearly basis to ensure compliance with latest standards and regulatory requirements. | CTO |

### 10.1.2 Key Management

| Sr. No | Activity | Responsible |
|---|---|---|
| 1 | Generate & use separate keys for different cryptographic systems | Network Administrator |
| 2 | Prepare detailed SOP for Key Management for cryptographic controls to ensure secure handling, generation, processing, maintenance & destruction by authorized persons that includes:<br>● Generating and obtaining public keys and distributing keys to intended users, including how keys should be activated when received<br>● Storing keys, including how authorized users obtain access to keys and changing or updating keys, including rules on when keys should be changed and how this will be done<br>● Dealing with compromised keys, revoking keys and specifying how keys should be withdrawn or deactivated<br>● Backup of keys, secure storage & retrieval of Backup keys. Recovering keys that are lost or corrupted as part of business continuity management<br>● Archiving, destroying keys<br>● Logging the auditing of key management-related activities<br>● Establishing defined activation and deactivation dates, limiting the usage period of keys, ensuring keys are changed frequently<br>● Physical & logical protection of equipment used to generate, | Application / System / Network Administrator |

| | | |
|---|---|---|
| | store and archive cryptographic keys<br>● Segregation of duties, with no single individual having knowledge of the entire cryptographic key (i.e. two-person controls) or having access to all the components making up these keys<br>● Ensuring no key ever appears unencrypted<br>● Ensuring keys that are transmitted are sent securely to well-authenticated parties<br>● Ensuring key-encrypting keys are separate from data keys.<br><br>And obtain approval from respective IT Heads | |
| 3 | Review and approve SOP for key management for cryptographic controls on yearly basis | IT Heads |
| 4 | Use secure channel to communicate the key between the encrypting and the decrypting system. If a secure channel is not available, then secondary channels are used to communicate the key/password separately from the message. | Application / System / Network Administrator |
| 6 | Communicate only Public key of an asymmetric key pair to intended user.<br><br>Do not communicate private key of an asymmetric key pair, ensure it is kept secret and stored securely<br><br>Maintain backup of an asymmetric key pair securely. | Application / System Administrator / End User |

# 11 Physical and Environmental Security

## 11.1 Secure Areas

### 11.1.1 Physical security perimeters

| Sr. No | Activity | Responsible |
|---|---|---|
| 1 | IBSL Office Premises.<br><br>IBSL IT Assets<br><br>IBSL environment is restricted and secured as follows:<br><br>● Visitor should not be allowed to the desk of officers<br>● Restricted areas to be accessible to designated employees only. | Admin |

### 11.1.2 Physical Entry Controls

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Train security staffs who manages physical access to the premises to discharge duties to meet the control objectives. | Admin |
| 2 | Maintain access register indicating the level of access given to the employee or third party and is updated regularly. | Admin |
| 3 | Authorize access to visitors for business purpose only. Supervise access provided to visitors | Admin |
| 4 | Record in and out time of the visitor along with purpose of visit and person whom he is visiting & new joiners. | Admin |
| 5 | Issue a visitor badge and record the visitor's badge number in the register and direct the visitor to wear the badge. | Admin |
| 6 | The visitor badge is returned. | Admin |
| 7 | Visitors are accompanied by an employee inside the restricted zone | Admin |

### 11.1.3 Securing Offices, Rooms and Facilities

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Admin personal of IBSL will determine the type and nature of security, security agency and the number of security guards required to be deployed at premises. | Admin |
| 2 | The security will protect the office area against all hazards like fire, malicious damages, theft, robbery etc. with integrity and sincerity. They will be alert during duty hours. | Admin |

### 11.1.4 Protecting Against External and Environmental Threats

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Lock the secure areas and access is controlled through automatic devices. | Admin |
| 2 | Use manual register for entering in the server room and the key is maintain at security. Authorization is given as define by CTO. | Admin / CTO |
| 3 | Proper air conditioning with temperature and humidity control is installed. | Admin |
| 4 | Do not allow food and drinking materials in secure areas. Smoking is strictly restricted. | Admin |
| 5 | Fire extensor system is in place at secure areas. Regular maintenance and checking is done for availability. | Admin |

### 11.1.5 Working in Secure Areas

⇒ Physical protection and guidelines for working in secure areas.

**Access to Data Servers and others**

⇒ Only the IT personnel deployed at the secure area will have access to server room.

⇒ Security will maintain a key register where he will mention the date, time and reason for which the IT person accessed the server room.

### 11.1.6 Delivery and Loading areas

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Register incoming and outgoing materials and no movement outside or inside IBSL premises should take place without authorization. | Admin |
| 2 | Register incoming materials on entry to site and delivery material is stamped | Admin |
| 3 | Do not provide access to delivery staffs to restricted zones in IBSL premises. | Admin |
| 4 | Inspect incoming material for potential hazard materials before they are moved to restricted zones | Admin |

### 11.1.7 Physical security Measures during Pandemic period

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Employees shall be allowed to work from home. Employees attaining office need to give self-declaration about self and family members. | Admin |
| 2 | Security measures is implemented to keep a clean and safe office environment:<br><br>a) Complete Sanitization of entire office on regular basis<br>b) Seating arrangement keeping safe distance<br>c) Sanitizer made available throughout the office,<br>d) All doors are kept open to avoid human touch,<br>e) AC Temperature of office maintained above 24 degree | Admin |
| 3 | Peoples coming to office shall be checked for a) Human body temperature b) biometric shall not be used till normalcy resumes. | Admin |
| 4 | Other Security measures: f) guest/vendor/clients/visitors shall be controlled to enter, g) flexible office hours, h) lunch time segregations, i) attendee at washroom gate for controlling congestion, | Admin |

## 11.2 Equipment security

To protect equipment's from physical and environmental threats to prevent loss, damage, theft or compromise of assets and interruption to the IBSL's activities.

### 11.2.1 Equipment siting and protection

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Equipment should be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. | Admin / Business Owner |
| 2 | Lock the secure areas and access is controlled through automatic devices | Admin |
| 3 | Use manual register for entering in the server room. Authorization for entry is given by CTO. | Admin / CTO |

### 11.2.2 Supporting utilities

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Primary and secondary backup ups power supply is installed. | Admin |
| 2 | Uninterrupted power supply system with adequate capacity is in place and is tested for its availability. | Admin |

### 11.2.3 Cabling security

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Power and communication lines are underground and are out of the reach of pests. | Admin |
| 2 | Power cables are separated from telecommunication cables to prevent interferences. | Admin |

| | | |
|---|---|---|
| 3 | Network communication lines are protected from unauthorized interceptions and damages. | Admin |

### 11.2.4 Equipment maintenance

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Maintain equipment under warranty or maintenance contract for continuous availability and integrity. | Admin |
| 2 | Maintain record of maintenance activities with the corrective and preventive actions. | Admin |

### 11.2.5 Removal of assets

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Equipment, information or software should not be taken off-site without prior authorization. | Admin / IT Head |
| 2 | Monitor all equipment movement within and outside the secure areas to mitigate the risks of unauthorized removal of equipment both by employees or any external personnel. | Admin / IT Head |

### 11.2.6 Security of equipment and assets off premises

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Obtain authorisation for use of any equipment outside an organization’s premises for information processing. | Business Owner / IT Head |
| 2 | Do not leave equipment and media taken off the premises unattended in public places. Portable computers are carried as hand luggage and disguised where possible when traveling. | End User |
| 3 | Manufacturers' instructions for protecting equipment are observed at all times, e.g. protection against exposure to strong electromagnetic fields. | End User |
| 4 | In case of theft, accidental damage of equipment’s decision related to re- | CTO |

| | | |
|---|---|---|
| | cover will be with CTO | |

### 11.2.7 Secure disposal of reuse of equipment

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | All equipment containing storage media should follow the destruction/disposal procedure as defined in handling procedure. | Admin |
| 2 | All equipment shall be re-used by ensuring that any sensitive data has been deleted prior to re-use | IT Infra Team |

### 11.2.8 Unattended user equipment

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Users should unattended equipment has appropriate protection. | Admin |
| 2 | All users shall they lock their computer screens when they leave their workstations unattended for short duration | Respective User/IT Infra Team |
| 3 | All users should log-off their PCs when the session is finished and while leaving the office, perform a normal shutdown and switch off the power to the PC; not just switch off the monitor or screen. | Respective User/IT Infra Team |

### 11.2.9 Clear desk and clear screen policy

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | ● All users should adopt a clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities.<br>● Sensitive or critical business information on papers or on electronic removable storage media should be under lock and key when not required, especially when the office is vacated.<br>● Workstations should be screen locked or protected with a password-controlled screen saver to ensure clear screen.<br>● Incoming and outgoing mail (courier) points and unattended facsimile machines should be protected | User/ HR |

| | | |
|---|---|---|
| | ● Unauthorized use of photocopiers and other reproduction technology (e.g., scanners, digital cameras) should be prevented<br>● Documents containing sensitive or classified information should be removed from printers immediately | |

# 12 Operations Security Management

## 12.1 Operational Procedures and Responsibilities

### 12.1.1 Documented Operating Procedures

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Document application/system/network architecture for critical systems and obtain approval from respective IT Heads that contains:<br>● End to end transaction flow<br>● Interfaces and relationships with other systems<br>● System and Network architecture including ports and services used | Developers & IT Infra Team |
| 2 | Document standard operating procedures (SOPs) for administration of IRIS and ensure adherence to the same and obtain approval from respective IT Head. | Developers & IT Infra Team |
| 3 | Store all application/system/network architecture and SOP documents it is available to relevant users of IRIS at any given time. | IT Infra Team / Development team |
| 4 | Review and update application/system/network architecture and SOPs on yearly basis and/or after any major changes and obtain approval from respective IT Head. | IT Infra Team |
| 5 | Maintain version control for modification of application/system/network architecture and SOP documents | Development Team & IT Infra Team |
| 6 | Approve standard operating procedure (SOPs) | CTO / Business Owner |
| 7 | Backup and maintain latest copy of standard operating procedure (SOPs) | IT Infra Team |

### 12.1.2 Change Management

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Changes to information processing facilities and systems follows 14.2.2. System change control procedures. Also refer Change Management procedure for IRIS. | Business Owner / PM / IT Head |

### 12.1.3 Capacity Management

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Monitor the use of resources for demand planning of future capacity requirements to ensure the agreed system performance is delivered. | Capacity Coordinator |
| 2 | Take into account the projections of future capacity requirements of new business and system requirements and current and projected trends in the IBSL's information processing capabilities. | Capacity Coordinator |

### 12.1.4 Separation of development, test and operational facilities

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Separate development, test, and operational facilities to reduce the risks of unauthorized access or changes to the operational system. | IT Infra Team |

## 12.2 Protection against Malwares

### 12.2.1 Controls against Malicious Code / Malwares

| Sr. No. | Description | Responsible |
|---|---|---|
| 1 | Deploy anti-malware solutions and keep it up to date to monitor and protect IBSL's information processing facilities against malware threats such as computer viruses, network worms, Trojan horses, spyware and logic bombs | IT Infra Team |
| Monitoring and Reporting | | |
| 1 | Anti-malware solution itself is up to date with the updates / patches and to its latest version. | IT Infra Team |
| 2 | desktops and laptops are up to date with anti-malware signatures;<br><br>All files and software downloaded/received either from or via external networks, mail, or on any other medium, are first scanned for viruses/malicious code etc., before being put to use. | IT Infra Team |
| 3 | Regular monitoring and review is done :<br>1) To ensure all the systems are up to date; | IT Infra Team |

| | | |
|---|---|---|
| | 2) To detect threats those are not contained by anti-malware solution.<br>3) To detect worm infections, in addition to monitoring of anti-malware solution monitor the logs from firewalls, intrusion detection and prevention sensors | |
| Remediation | | |
| 1 | Identify the infected systems which are not contained by the anti-malware solution.<br><br>Record security incident for identified outbreak of malware and follow security incident management procedure. | IT Infra Team |

## 12.3 Backup and Retention/Archival

### 12.3.1 Information backup

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Data backup, restoration and testing is outsourced to AWS. IRIS application and data is hosted on AWS data center. Application and data availability is ensured though High availability sites of AWS data centre.<br><br>Refer to IRIS – Backup Policy document. | AWS |

## 12.4 Logging and Monitoring

### 12.4.1 Event logging

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | **Logging Parameters/Fields -** Infra logs are generated containing Level, Date-Time, Source, Event ID and Task Category. Application logs are generated on server and the same are available for review to IRIS team. Firewall Logs included usage details, intrusion attempts alerts and prevention reports. The same are reviewed on quarterly basis. | CTO |

### 12.4.2 Protection of log information

| Sr No | Activity | Responsible |
|---|---|---|
| 1 | Access to logs are only with the authorized personnel. | CTO |

### 12.4.3 Administrator and operator logs

| Sr No | Activity | Responsible |
|---|---|---|
| 1 | Infra logs are generated containing Level, Date-Time, Source, Event ID and Task Category. Application logs are generated on server and the same are available for review to IRIS team. | Network Administrator |

### 12.4.4 Clock synchronization

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Establish a time server (NTP server) and synchronize with an external trusted authoritative time source as per Indian Standard Time (IST). This time server shall act as times source for all servers/systems/devices/PCs etc. within IBSL's. | IT Infra Team |
| 2 | Maintain continuous availability of a time server and synchronization with external authoritative time source. | IT Infra Team |
| 3 | Synchronize system clock of all servers/systems/devices/PCs etc. with a time server to ensure date and time is in sync with authoritative time source so that time stamps in logs are consistent. | IT Infra Team |

## 12.5 Control of Operational Software

### 12.5.1 Installation of software on operational systems

| Sr No | Activity | Responsible |
|---|---|---|
| 1 | Prepare the fall back plan for software installation. | Business Owner / PM |
| 2 | Identify respective personnel from the IT team who will be responsible for application installation | Business Owner / PM |
| 3 | After the software is approved in acceptance testing, install in production environment. In case of any incident, follow fall back plan. | Business Owner / PM |
| 4 | Test the installed application and provide sign-off | Business Owner / PM |

## 12.6 Technical Vulnerability Management

### 12.6.1 Management of technical vulnerabilities - Application Security

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Send advance notification prior to commencement of any type of application security assessment. | IT Head |
| 2 | Update asset list and inform IT Security Team | IT Infra Team |
| 3 | Conduct application security assessment | CTO / Third Party |
| 4 | Testing Approach:<br>▪ Every security testing consists of at least two cycles, Test and Retest.<br>▪ Re-test cycle to retest the closure of identified vulnerabilities of all previous assessments<br><br>Types of Testing:<br>▪ Internal & External Testing<br>▪ Black-box & Grey-box Testing<br><br>Frequency:<br>▪ Conduct application security assessment annually.<br>▪ Conduct network security assessment annually.<br><br>Reporting:<br><br>Ensure that the security assessment report to contain at minimum:<br><br>▪ IP Address<br>▪ Application / Asset Name<br>▪ Vulnerability name / description<br>▪ Impact<br>▪ Risk Rating<br>▪ Recommendations<br>▪ Identification Date of the vulnerability, which can be assessment date itself wherein the vulnerability is identified for the first time<br><br>Status indicating “Open”, “Closed” and “Exception” of the vulnerabilities identified | CTO / Third Party |

| | | |
|---|---|---|
| 5 | Post each application security assessment; submit the draft report to relevant stakeholders for their validation of coverage of assets under their control. | CTO / Third Party |
| 6 | Publish the final report to all relevant stakeholders. | CTO / IT Head |

### 12.6.2 Restrictions on software installation

| Sr. No. | Description | Responsible |
|---|---|---|
| 1 | Ensure the list of authorized software is maintained up-to-date.<br><br>Semi-annually review the list of authorized software and obtain approval from CIO/CTO | IT Infra Team |
| 2 | Only authorized software is installed on IRIS systems. | IT Infra Team |

### 12.6.3 Patch Management

| Sr. No. | Description | Responsible |
|---|---|---|
| 1 | All new patches will be prioritized based on factors such as nature of the patch, vendor criticality, risk to the un-patched system in current environment and any other applicable parameter. | IT Infra Team |
| 2 | Patches that require the information processing facility to be taken offline will not be applied during business hours. In case of emergency patches, the Security Officer and the information asset owner will approve implementation during the working hours after adequate communication to all the stakeholders and the IT users getting impacted. | IT Infra Team |
| 3 | Patches will be tested in a Dev/test environment prior to application in production systems. | IT Team |
| 4 | Once a patch is applied, it is necessary to assess the deployment and identify any issues that require mitigation. If any serious issues arise, IT team should follow the rollback plan to return the system to the pre-patch state. | IT Team |
| 5 | Periodic reviews will be done to assess if the Company's IT department information systems are patched with the latest appropriate patches. Such reviews will also take inputs from | CTO |

| | | |
|---|---|---|
| | technical vulnerability assessments conducted previously | |
| 6 | Patches should be downloaded from authorized source only. | IT Team |
| 7 | Frequency:<br>▪ Patching for all server and sensitive host should be scheduled after every 30 days. This accommodates critical patches released by vendors such as Microsoft.<br>▪ Patching for all Workstation should be scheduled after every 30 days. | IT Team |

## 12.7 Information Systems Audit Consideration

### 12.7.1 Information systems audit controls

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | An annual review assesses the adequacy of information system controls and compliance with ISMS controls.<br><br>An internal audit for the Information Systems is conducted every 12 months to ensure that adequacy is maintained in the design and operations of the IT systems. All high/critical observations arising from the internal audit are mitigated within 3 months. | CTO |

## 13 Communications Security Procedure

**Objective**
To ensure the protection of information in networks and the protection of the supporting infrastructure.

**Procedure**

### 13.1 Network security management

### 13.1.1 Network Controls

| Sr. No | Activity | Responsible |
|---|---|---|
| 1 | Assess the need for allowing access to IBSL's network from specific locations and equipment's. Identify the types of network access requiring restriction on equipment used for access. | IT Infra Team |
| 2 | Access to identified critical devices like routers, firewalls is restricted only to the authorized personnel. | IT Infra Team |
| 3 | Determine mechanism for implementing the network perimeter controls for segregating networks.<br><br>IBSL User asset & servers are differentiated using different IP segment | PM/ CTO |
| 4 | Implement firewall at the perimeter level. | IT Infra Team |
| 5 | Ensured that all wireless communication is uses strong authentication. Production environment is on AWS, Azure or Client's environment hence wireless network not be enabled for production. | IT Infra Team |

### 13.1.2 Security of network services

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Based on user / application access requirements identify network access requirements (source IP address, destination IP address, destination port number / service required) to information systems and network services. | IT Infra Team |
| 2 | Follow the Change Management Policy and Procedure for the implementation of network access. | IT Infra Team |

### 13.1.3 Segregation in networks

| Sr.No. | Activity | Responsible |
|---|---|---|
| Developing Network Diagram | | |
| 1 | Developed Network diagram by including the following details at minimum:<br>● Network architecture<br>● All critical network equipment's, along with their IP addresses<br>● All critical communication links (primary as well as standby)<br>● Wireless networks, if any | IT Infra Team |
| 2 | The Network Diagram should be reviewed and approved. | CTO/IT Head |
| Maintaining Network Diagram | | |
| 1 | Review the network diagram on a semi-annual basis. | IT Head / CTO |
| 2 | The Network Diagram should be updated in case there is:<br>● Addition of new equipment /s<br>● Major change done in the network | IT Infra Team |

## 13.2 Information transfer

### 13.2.1 Information transfer policies and procedures

| Sr No | Activity | Responsible |
|---|---|---|
| 1 | Following measures are taken to protect information exchange :<br><br>All information exchange devices such as end point routers, VPN gateways and other network devices follows security controls as described in the "network security management" section of this document. | IT Infra Team |
| 2 | For every instance of the business information exchange, explicit approval to be obtained from the Business Owner of that application or his delegate. | End User / Line Manager |

### 13.2.2 Agreements on information transfer

- Executed copy of agreement will be handed over to CFO/finance

### 13.2.3 Electronic Messaging & Instant Messaging

| Sr No | Activity | Responsible |
|---|---|---|
| 1 | All email communications are secured as per the following IS procedures | IT Infra Team |
| 2 | Stop access for all Internet Email Systems like Hotmail, Rediffmail, YahooMail, etc and file sharing. | IT Infra Team |

### 13.2.4 Confidentiality or non-disclosure agreements

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Identify requirements related to confidentiality and non-disclosure for protection of information accessible by third parties and incorporate in the Non-Disclosure Agreement for implementation.<br><br>Also review the confidentiality and non-disclosure agreements whenever there is change in the service terms and conditions or change in the regulatory / legislation. | CTO/CIO |

# 14 System Acquisition, Development and Maintenance Procedure

**Objective**
To security is an integral part of information systems in system acquisition, Development & Maintenance.

**Procedure:**

## 14.1 Security Requirement of Information Systems

### 14.1.1 Information security requirement analysis

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Assess, Identify and agree security requirements / controls for :<br>● New systems / technology<br>● Major Enhancements in existing systems / technology<br>● Business operation/s to be outsourced<br>● Vendor / Third party involvement | IT Head / CTO / PM |

### 14.1.2 Securing application services on public networks

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Secure access to IRIS in terms of public & private key. | IT Infra Team |

### 14.1.3 Protecting application services transactions

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | IRIS Product services are hosted on AWS cloud and Azure Cloud & contractual agreement is in place to protect application services transactions. | AWZ & Azure services / PM |

## 14.2 Security in development and support process

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Security in development & support processes | Development Team |

### 14.2.1 Secure deployment policy

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Deployment of source code will be moved to production after testing on test server (UAT). | Development Team |

### 14.2.2 System change control procedures

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Change requests shall be documented and include:<br>a) Approval from respective business owner /PM<br>b) Approval from implementer's manager (IT Head / PM)<br>c) Approval from Chief Information Officer (CIO / Business Owner) | IT Infra Team / PM / Business Owner / Customer / QA |
| 2 | Approval of the change requests shall be based on:<br>a) Need for change<br>b) Impact of change on applications and dependent systems<br>c) Priority of change<br>d) Security implications<br><br>There shall be implementation plan (POA) for implementing a change that includes:<br>a) Pre-requisites (if any)<br>b) Implementation steps<br>c) Time and resource requirements<br>d) Downtime requirements, if any<br>e) Test plan<br>f) Fall-back plan<br>g) Roll back plan<br><br>All changes shall be monitored and reviewed for successful implementation.<br><br>Refer to the IBSL - Change Management Procedure document. | IT Infra Team / PM / Development Team. |

### 14.2.3 Technical review of applications after operating platform

| Sr No | Activity | Responsible |
|---|---|---|
| 1 | Prepare the fall back plan for software installation. | Business Owner |
| 2 | Identify respective personnel from the IT team who will be responsible for application installation | Development Team |

| | | |
|---|---|---|
| 3 | After the software is approved in acceptance testing, install in production / Deployment environment. In case of any incident, follow fall back plan. | System Administrator |
| 4 | Test the installed application and provide sign-off | Business Owner |

### 14.2.4 Restriction on changes to software packages

| Sr No | Activity | Responsible |
|---|---|---|
| 1 | Restrict modification of vendor supplied software packages as far as possible and practicable | IT Infra Team / PM |
| 2 | Any changes requested follows change procedure. | IT Infra Team / PM |
| 3 | If changes are essential, then original software is retained and the changes will be applied to a clearly identified copy. While executing the changes, care will be taken to avoid the possibility of compromising the built in controls. | IT Infra Team / PM |
| 4 | Where it is deemed essential to modify vendor supplied software package, follow the below aspects:<br>● An assessment of built-in controls and integrity processes, which may be compromised due to the changes, are made.<br>● Consent of the vendor for the modifications are obtained wherever possible.<br>● The possibility of obtaining the required changes from the vendor as standard program updates.<br>● Impact on the future maintenance and warranties of the software as a result of changes and modifications should be assessed.<br>● All changes are fully tested and documented, so that they can be reapplied if necessary to future software upgrades. | Change Manager |

### 14.2.5 Secure system engineering principles

| Sr. No. | Activity | Responsible |
|---|---|---|

| | | |
|---|---|---|
| 1 | Ensure that secure system engineering principles are followed in software development | Development Team |

### 14.2.6 Secure development environment

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Identified developed code must be protected from theft, stolen etc.<br><br>SOD has been defined for developer, BA, Testing team, PM | PM |

### 14.2.7 Outsourced Development

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Agreement should be in place to protect developed code which is outsourced to third party | PM |

### 14.2.8 System Security Testing

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Periodic System Security must take place. | CTO / CIO |

### 14.2.9 System Acceptance Testing

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Maintain development, test and production environments separately and all technical documentation is updated to reflect the changes. | IT Infra Team / Development team |
| 2 | Establish acceptance criteria for new information systems, upgrades, and new versions and suitable tests of the system(s) carried out during development and prior to acceptance. | PM / Business Owner |
| 3 | Identify the risk of any deviations to acceptance criteria's and accept/approve the same as per Risk Management Procedure | CTO/ HRM |
| 4 | Perform unit testing upon completion of development activities and update the same in Change Management system. | PM / Business Owner |
| 5 | Perform an independent review of the test result and formally sign-off on the test results. | PM / Business Owner |

| | | |
|---|---|---|
| 6 | Conduct integration testing in a separate, independently controlled test environment where developers will have no access to this environment. | QA / UAT Team |
| 7 | The concerned divisions / users will indicate acceptance through formal sign-off. | PM |
| 8 | If defects are noted, document the defects and make appropriate modifications and submit it to the Quality Assurance for retesting. | QA Team |
| 9 | Perform acceptance testing and approve the changes before moving it into production environment. | QA Team |
| 10 | The program and configuration changes are tested in the test environment and the roll back procedures are defined by the IT team. | IT Infra Team / PM |
| 11 | If the UAT is approved by the business user, change request is raised for implementing the change in the production server. | PM |
| 12 | The production server change goes through the normal process of change approval till live proving. | Business Owner |

## 14.3 Test Data

### 14.3.1 Protection of test data

| Sr No | Activity | Responsible |
|---|---|---|
| 1 | Store the test data in access controlled test environment. | PM |
| 2 | Ensure non-disclosure agreement is arranged with third party vendor if customer data is shared for testing. | PM / Business Owner |
| 3 | Encrypt the test data if it contains customer details. | PM / Development Team |
| 4 | Destruct/ remove the sample data after successful testing... Request the vendor to remove the data once testing is completed. | PM / Business Owner |

# 15 Supplier Relationships

**Objective**

Procedure to define supplier relationship management

**Procedure:**

## 15.1 Information Security in Supplier Relationships

### 15.1.1 Information security policy for supplier relationships

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Information security requirements for mitigating the risks associated with supplier's access to the organization assets shall be agreed with the supplier and document | CTO |

### 15.1.2 Addressing security within supplier agreements

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | The agreement between IBSL and the third parties including the sub-contractor if any should specify the security considerations to be addressed.<br><br>The security requirements should address exchange of information through all forms of communication. | CIO / CTO |
| 2 | The agreements should address the requirements with third parties including the sub-contractors, as applicable. | Business Owner / IT Head |
| 3 | Applicable confidentiality, non-disclosure and security requirements should be signed off | Business Owner / IT Head / Third Party |
| 4 | Each contractor (user) and third party service provider enters into a confidentiality and non-disclosure agreement with the IBSL before commencement of engagement. | Business Owner / IT Head |
| 5 | In case of termination, it should be ensured that third party access to IBSL's information systems is removed as per the defined procedure for removal of access rights. | Business Owner / IT Head |
| 6 | In case of termination, it should be ensured that the confidential information with the third party, as well as subcontractors, is | Business Owner / IT Head |

| | | |
|---|---|---|
| | returned/ destroyed as per the terms of agreement. | |

### 15.1.3 Information and communication technology supply chain

| | | |
|---|---|---|
| Confidentiality or Non-Disclosure Agreements | | |
| 1 | Identify requirements related to confidentiality and non-disclosure for protection of information accessible by third parties and incorporate in the Non-Disclosure Agreement for implementation.<br><br>Also review the confidentiality and non-disclosure agreements whenever there is change in the service terms and conditions or change in the regulatory / legislation. | CIO |
| 2 | Confidentiality or non-disclosure agreements should be renewed every year. | Business Owner / IT Head |
| Identification of Risks Related to External Parties | | |
| 1 | Determine the list of security controls to be implemented based on the type of engagement and nature of information sharing requirement at IBSL's end as well as third party. | IT Infra |
| 2 | Exceptions, if any should be sought as per the Risk Management | Business Owner / IT Infra Head |

## 15.2 Supplier Service Delivery Management

### 15.2.1 Monitoring and review of supplier services

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | The services, reports and records provided by the third party should be reviewed at least once a year | IT Infra Head/Business Owner |

### 15.2.2 Managing changes to supplier services

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Risk assessment to determine the security risk that should be carried out before making changes to the provision of services as per risk management procedure | IT Delivery Head/Business Owner |
| 2 | Due diligence to ensure security requirements are addressed as per information systems procedure | IT Infra Head/Business |

# 16 Information Security Incident Management

**Objective**
Procedure to define Information Security Incident Management

**Procedure:**

## 16.1 Management of Information Security Incidents and Improvements

### 16.1.1 Responsibilities and procedures

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Responsibilities and procedures should be sufficiently defined for incident management. | IT Head/CTO |

### 16.1.2 Reporting information security events

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Report / Notify any information security event in systems or services to IT Infra team.<br><br>Security Incidents may be reported through telephone calls, voice mails, visit's, letters or e-mails. | Incident Notifier |
| 2 | Verify the notification to determine if it is a valid security incident or not.<br><br>In case of invalid security incidents, inform the incident notifier. | IT Infra Team |
| 3 | For valid security incidents, provide confirmation to the notifying process/ incident notifier. | IT Infra Team |

### 16.1.3 Reporting information security weaknesses

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Report / Notify any information security event in systems or services to IT Infra team.<br><br>Security Incidents may be reported through telephone calls, voice | Incident Notifier |

| | | |
|---|---|---|
| | mails, visit's, letters or e-mails. | |
| 2 | Verify the notification to determine if it is a valid security incident or not.<br><br>In case of invalid security incidents, inform the incident notifier. | IT Infra Team |
| 3 | For valid security incidents, provide confirmation to the notifying process/ incident notifier. | IT Infra Team |

### 16.1.4 Assessment and decision on information security events

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Review all relevant information relating to the nature of the incident. Further details or clarification (if any) should be obtained from the incident notifier. | IT Head/CTO |
| 2 | Classify the security incident based upon the below defined priority criteria/guidelines. The details should be recorded. Multiple events may relate to one security incident. Such events should be recorded as a single security incident.<br><br>Classification/Priority is as follows :<br><br>1) High Priority : High business impact<br><br>2) Medium Priority : Moderate business impact<br><br>3) Low Priority : Low business impact | Requestor/ IT Infra Team |
| 3 | Incident wherein the server or application is affected severely will be considered for incident management process. End user related incidents are carved out of the process. | Requestor/ IT Infra Team |

### 16.1.5 Response to information security incidents.

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Security incidents should be responded promptly and the response should be in line with the classification of incident. | IT Infra Team |

### 16.1.6 Learning from information security incidents

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Prepare service reports based on the data collected for the recorded security incidents. The service report should highlight the performance metrics to enable management review and should exhibit information on both the detailed status of incidents and the overall state of Security Incident Management. | IT Infra Team |
| 2 | Review the Incident Records and update the status of security incidents to the stakeholders. | IT Infra Team |
| 3 | Review learning's from the security incidents and identify actions for preventing the recurrence of similar incidents on a regular basis.<br><br>Updates from Professional Associations and Security Forums should be obtained and considered in determining the preventive actions. | IT Infra Team / IT Head/CTO |

### 16.1.7 Collection of Evidence

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Incident evidence should be identified, collected, acquired and preserved in a manner that the same can be used as reference. | IT Infra Team / IT Head/ CTO |

# 17 Information Security Aspects of Business Continuity Management

## 17.1 Information Security Continuity

### 17.1.1 Planning information security continuity

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Identify business processes that are critical for the continuity of IBSL's IRIS operations | BCP coordinator |
| 2 | Information Security events that can cause interruptions to business will be identified and assessed to determine their impact | BCP coordinator |
| 3 | Carry out a detailed Risk Analysis and Business Impact Analysis ('BIA') to identify IS events that are critical for the continuity of IBSL's IRIS operations | BCP coordinator |
| 4 | Identify Recovery Time Objectives (RTO's) for each of the resources, based on their criticality and taking into consideration process/system interdependencies.<br><br>IRIS Product Applications are hosted on AWS and Azure which is ensuring data availability and application connectivity. RTO is real time and the same is ensured through uptime commitment. | BCP Committee |
| 5 | Perform the above-mentioned risk assessment at least on an annual basis, to the BIA and RTO's are in line with changing business operations and requirements. | BCP Committee |
| 6 | Develop framework of business continuity plan based on the priorities identified.<br><br>Business application is maintained by AWS and Azure which ensures high availability of application. | BCP Committee |

### 17.1.2 Implementing information security continuity

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | The outcome of the BIA is used for prioritising resource availability and developing the actual BCP.<br><br>As part of the BCP development process, the adequacy of the security requirement for current availability practices will be evaluated vis-à-vis the identified RTOs. If the current practices are inadequate, | BCP Committee |

| | | |
|---|---|---|
| | IBSL will identify various alternative continuity options with the objective of selecting a strategy that best meets its recovery requirements.<br><br>The extent of business operations that should, at a minimum, be made available in the event of a contingency should be identified. The BCP must take into account this requirement during the course of identification of the best recovery strategy. | |

### 17.1.3 Verify, review and evaluate information security continuity

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | The BCP will be tested at least on a half yearly basis.<br><br>The details and results of the testing will be recorded and used as input for evaluating the effectiveness of the BCP and the necessity for updating, if any.<br><br>The BCP will be reviewed and updated, if necessary, on an annual basis to it is current and takes into account, modified business circumstances | BCP Committee |

## 17.2 Redundancies

### 17.2.1 Availability of information processing facilities

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.<br><br>Since AWS and Azure is maintaining IRIS Product systems, availability of the same is ensured through uptime commitment. | BCP Committee |

# 18 Compliance

## 18.1 Compliance with Legal and Regulatory Requirements

### 18.1.1 Identification of applicable legislation and contractual requirements

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Requirements related to applicable statutory acts to IBSL IRIS SOFTWARE Product information system are defined, documented as follows;<br>● Information Technology Act 2010<br>● Companies Act<br>● Contract Labor Act 1970<br>● Payment of Wages Act 1936<br>● Minimum Wages Act 1948<br>● Industrial Establishment (National and Festival Holidays) Act<br>● Labor Welfare Fund Act<br>● Employees State Insurance (General Regulations) Act 1952<br>● Maternity Benefit Act 1961<br>● Equal Remuneration Act 1976<br>● Income Tax Act | Legal Co-ordinator |

### 18.1.2 Intellectual property rights (IPR)

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | IBSL will not infringe the copyrights and intellectual property rights of others and will not use such materials without required permissions.<br><br>Only that software which is licensed to the company will be used in accordance with the given terms and conditions.<br><br>Licenses agreements and other evidences of purchase product will be maintained in secure place.<br><br>Any material developed by the organization will only be used after approval.<br><br>Employees will not violate any copyrights through their actions. | Legal Co-ordinator |

| | | |
|---|---|---|
| | Employees should not use any Company's asset for violating copyrights | |

### 18.1.3 Protection of Organizational Records

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Wherever electronic storage media are chosen, the ability to access data throughout the retention period will be clearly defined and suitable safeguarding against loss due to technology change will be addressed. | Developers |
| 2 | Record will be retained securely as per the statutory, regulatory or business requirement. | Developers |
| 3 | Records kept in soft form will have sufficient back up stored as per the backup procedure. | Developers |
| 4 | All records will be indexed and cross-referenced wherever applicable for easy identification and retrieval. | Developers |

### 18.1.4 Privacy and protection of personally identifiable information

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Personally identifiable information should be identified and protected from loss or theft. | CTO |
| 2 | Data received via email, whether PII or Non-PII, for debugging or troubleshooting purposes from client, is promptly and securely deleted | Team Leader |

### 18.1.5 Regulation of cryptographic controls

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations. | Business Application Owners / IT Heads |

## 18.2 Information Security Reviews

### 18.2.1 Independent review of information security

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Independent reviews should be planned at the frequency stated in the ISMS manuals, on the basis of the status and importance of the activity to be audited. The frequency of the audits should be increased based on internal/external non-conformance, customer complaints and verification of corrective/preventive action effectiveness during follow-up audit. | CTO |
| 2 | The audits should compare actual practices to the documented procedures listed in the ISMS Procedure Manual. | CTO |
| 3 | Audits should verify the compliance to ISMS objectives and action plan, thus evaluating the ability of the process to achieve results. | CTO |
| 5 | The CTO should arrange for independent audit as per the planned schedule and program. | CTO |
| 7 | It is the responsibility of the auditee to get these non-conformities adequately resolved and get the clearance of the Auditors. The auditee sends a copy of the closed non-conformity report to CTO. | CTO |
| 8 | Management Audit reports should be reviewed by CTO and non-conformances compiled. | CTO |

### 18.2.2 Compliance with security policies and standards

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | Managers shall review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements on annual basis. | Business Application Owners / IT Heads |

### 18.2.3 Technical compliance review

| Sr. No. | Activity | Responsible |
|---|---|---|
| 1 | IT Security and Application Security shall be reviewed on semi-annual basis with the organization's information security policies | CTO |

| | | |
|---|---|---|
| | and standards. | |

**End of Document**