Bharti Infratel

Information Security & Business Continuity Policy- Abridged

(BIISBCP-Abridged)

Version 4
### A. Document Control

<table>
<thead>
<tr>
<th>S No</th>
<th>Type of Information</th>
<th>Document Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Document Title</td>
<td>Bharti Infratel Information Security &amp; Business Continuity Policy – Abridged</td>
</tr>
<tr>
<td>2</td>
<td>Version No.</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>Date of Release</td>
<td>16-Dec-19</td>
</tr>
<tr>
<td>4</td>
<td>Document Owner</td>
<td>Mr. Dipak Roy</td>
</tr>
<tr>
<td>5</td>
<td>Document Author</td>
<td>Mr. Abnish Bhargava</td>
</tr>
<tr>
<td>6</td>
<td>Document Approver</td>
<td>Mr. Dipak Roy</td>
</tr>
</tbody>
</table>

### B. Document Change Approvals

<table>
<thead>
<tr>
<th>S No</th>
<th>Version No.</th>
<th>Nature of Change</th>
<th>Approval Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>Integrated ISBC policy released as part of integration of ISO 22301 and ISO 27001 and the migration from ISO 27001:2005 to ISO 27001:2013.</td>
<td>5th November 2015</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>Annual review</td>
<td>30-Oct-17</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>Annual review &amp; document owner &amp; approver change</td>
<td>30-Apr-2018</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>Changes in Owner, Author &amp; Approver. Annual Review</td>
<td>16-Dec-19</td>
</tr>
</tbody>
</table>

### Disclaimer

This is an internal and proprietary document of Bharti Infratel Limited and should not be copied or disseminated to any one not authorized to receive it. Accordingly, this document may not be disclosed, used or duplicated - in whole or in part - for any purpose other than the sole purpose of facilitating Information Security and Business Continuity at BIL.
# Table of Contents

1. Introduction .................................................................................................................. 5  
   1.1 Management Intent .................................................................................................. 5  
2. Scope ........................................................................................................................... 6  
   2.1 Definitions ............................................................................................................. 6  
   2.2 Policy Owner and Approver ................................................................................ 7  
   2.3 Roles of key stakeholders for Policy Enforcement ............................................. 7  
   2.4 ISBC Policy document ......................................................................................... 8  
   2.5 Consequence Management for Non-Compliance ............................................. 8  
   2.6 ISBC Roles & Responsibilities ......................................................................... 8  
3. Information Security & Business Continuity Policies ............................................. 8  
   3.1 Organization of ISBC ......................................................................................... 10  
4. Mobile device and Teleworking policy ................................................................. 11  
5. Human resource security policy ........................................................................... 12  
6. Asset Management ................................................................................................. 13  
7. Access Control .......................................................................................................... 15  
8. Cryptography ........................................................................................................... 17  
9. Physical & Environmental Security ....................................................................... 17  
10. Operations Security ................................................................................................ 18  
11. Communications Security ................................................................................... 19  
12. System acquisition, development and maintenance .......................................... 21  
13. Supplier Relationships ......................................................................................... 21  
14. Information security incident management ....................................................... 22  
15. Information Security aspects of business continuity ......................................... 23  
16. Compliance ............................................................................................................. 24
Policy Statement

“Bharti Infratel Limited shall ensure protection of information, safety of its people and continuity of business operations from key threats identified, whether internal or external, deliberate or accidental, such that the brand is protected; confidentiality of information is maintained; integrity of information can be relied upon and availability of information is ensured; in order to support delivery of key services to its customers, while abiding to legal, regulatory and contractual obligations, by developing, implementing and continually improving an organization wide Information Security and Business Continuity Management System.”
1. Introduction

Information Security and Business Continuity Management System (ISBC MS) lays down a risk management framework which establishes, implements, operates, monitors, reviews, maintains and continually improve information security and business continuity (ISBC) at Bharti Infratel Limited (hereafter referred as BIL).

Bharti Infratel Information Security and Business Continuity Policy (hereafter referred as BIISBCP) of BIL that its information is comprehensively protected against the consequences of breaches of confidentiality, failures of integrity, interruptions to their availability, loss of authenticity and/or repudiation of a transaction. This is supported by a business continuity management framework which provides an overall strategy to ensure continuity of key business operations during crisis situations. The structure of policy has been aligned to the structure of the ISO 27001:2013 and ISO 22301:2012 an overall management system standard for Information Security& Business Continuity:

1.1 Management Intent

The BIISBCP document defines BIL’s position on information security and business continuity. The BIL management has approved and published this policy to set a clear corporate direction and demonstrate support for, and commitment to information security and business continuity. The BIISBCP provides management direction and support to ensure the protection of its information and to allow access, use and disclosure of such information in accordance with appropriate standards, laws and regulations across functions and locations in scope.

The Information Security and Business Continuity Steering Committee (ISBC SC) shall demonstrate its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISBC MS by:

a. Establishment of BIISBCP and objectives in line with the organization objectives;

b. Establishment of an ISBC MS governance structure, highlighting roles and responsibilities;

c. Identification of internal and external interested parties and performing risk and opportunities assessment with respect to the context of organization;

d. The management shall determine the criteria for accepting risk and acceptable levels of risk followed by development of risk treatment plans. Risk treatment plans shall also assist in development of recovery strategies for the critical business activities identified;

e. Communicating to the organization the importance of meeting information security and business continuity objectives and conforming to the BIISBCP;
2. Scope

The BIISBCP is applicable to all information owned and managed by BIL. An information is a definable piece of information, stored and/ or processed in any manner, which is recognised as valuable to the organisation. The information contained in asset could be classified as software, physical (hardware), paper, people and information that are physically or electronically stored, processed and/ or transmitted. The BIISBCP is applicable to all employees including associates working out from BIL premises. All ISBC adherence requirements for third parties (classified as strategic partners) of BIL shall be governed by this policy.

As a reference of this document, a service provider is called a Third-party only after association with BIL. These third parties are strategic partners who enter into direct contracts with BIL for providing products or services. They also include vendors to whom the strategic partners may have outsourced or sub-contracted the delivery of products or services that the strategic partner are required to provide to BIL. Third parties include IT service providers (e.g. IBM) and their sub-contractors, consultants, representatives etc.

The BIISBCP is applicable across all functions and geographies in scope where the information assets of BIL are located or as appropriate.

2.1 Definitions

Information Security refers to the safe-guarding information and information systems from unauthorised access, modification, use, disruption and destruction to ensure availability, confidentiality, integrity, authenticity and non-repudiation of information. Business Continuity means
strategic and tactical capability of the organisation to plan for and respond to incidents and business disruptions in order to continue operations at an acceptable predefined level.

2.2 Policy Owner and Approver

The author of the BIISBCP- Abridged is the Management Representative (hereinafter referred to as MR). The MR shall be responsible for the maintenance and update of the BIISBCP - Abridged document. The BIISBCP - Abridged is approved by the CISO (Chief Information Security Officer).

2.3 Roles of key stakeholders for Policy Enforcement

a. Strategic

Information Security and Business Continuity Steering Committee (ISBC SC)

The ISBC SC constitutes of all the executive council members, shall be accountable for enforcing the implementation of the BIISBCP.

b. Circle

The Circle Business Head shall be accountable and responsible for overseeing all aspects related to security operations, business continuity readiness and shall drive overall ISBC at respective circles.

c. Chief Information Security Officer (CISO)

The CISO shall be responsible for ensuring that policies constituting the BIISBCP are current and reflect the requirements of BIL.

d. Information Security and Business Continuity Core Group (ISBC CG)

The ISBC CG shall be responsible for enforcing the implementation of relevant BIISBCP clauses (as applicable).

e. Information Security Business Continuity Management Representative (ISBC MR)

The ISBC MR shall be responsible for overseeing all aspects related to security and continuity operations and driving overall ISBC arrangements at BIL.

f. All Employees

It is the responsibility of all employees to read, understand and adhere to the BIISBCP.

g. All Strategic Partner Staff /Associates

As part of contractual requirement, it is the responsibility of all strategic partner staff and associates to understand and adhere to the BIISBCP. The right to audit clause is also embedded in the contract as appropriate.
2.4 ISBC Policy document

The BIISBCP provides management directive for ISBC and recommends appropriate security and continuity controls that need to be implemented to maintain and manage the information security and business continuity at BIL. The BIISBCP shall be communicated throughout the organization to users in a form that is relevant, accessible and understandable to the intended audience.

2.5 Consequence Management for Non-Compliance

All employees, associates and strategic partner staff are required to comply with the BIISBCP as applicable. Non-compliance with the BIISBCP is ground for consequence management, and shall be dealt with as per organisational Bharti Infratel Limited Policy on Consequence Management for breach of Code of Conduct (Financial & Non-financial Impropriety)

2.6 ISBC Roles & Responsibilities

The ISBC roles and responsibilities shall be defined and assigned at all levels to ensure that the assigned individuals understand the significance of their roles.


Policy Statement:

“Bharti Infratel Limited shall ensure protection of information, safety of its people and continuity of business operations from key threats identified, whether internal or external, deliberate or accidental, such that the brand is protected; confidentiality of information is maintained; integrity of information can be relied upon and availability of information is ensured; in order to support delivery of key services to its customers, while abiding to legal, regulatory and contractual obligations, by developing, implementing and continually improving an organization wide Information Security and Business Continuity Management System.”

The ISBC MS objectives at BIL are:

a. To provide a safe working environment for human resources;

b. To establish robust information security and business continuity management framework related risks, by performing threat assessment and identification of risks associated with information assets along with recovery strategies for process resumption within identified timelines to achieve minimum business continuity objective;
c. To establish an information security and business continuity governance framework and ensuring its alignment to key business objectives;

d. To comply with the statutory, regulatory and contractual requirements as applicable;

e. To implement mechanisms to ensure that information security breaches and business continuity incidents are reported and appropriately investigated followed by adequate actions;

f. To create and maintain awareness of information security and business continuity practices across organization;

g. To establish, implement, maintain and continually improve information security and business continuity management system.

The BIISBCP provides management directive for ISBC and recommends appropriate security and continuity controls that need to be implemented to maintain and manage the information security and business continuity at BIL. The BIISBCP shall be communicated throughout the organization to users in a form that is relevant, accessible and understandable to the intended audience.

The policy shall explain the policies, principles and compliance requirements for particular importance to the organization, including:

   a. Legislative, regulatory, and contractual compliance;

   b. Security education, training, and awareness requirements;

   c. Business continuity management; and

   d. Consequences of information security policy violations.

The BIISBCP document (including all policies referred as part thereof) shall be reviewed at the time of any major change(s) in the existing business environment affecting policies and procedures or at least once every year, whichever is earlier.
3.1 Organization of ISBC

The organization of ISBC MS shall be enforced by:

a. Establishing a management framework to initiate and control the implementation of ISBC within the organization;

b. Ensuring that a governance framework is developed to maintain ISBC within the organization; and

c. Assigning the security roles, pre crisis, during crisis and co-ordinating the implementation of security and continuity across the organization.

d. Segregation of duties is required so that no single user has the ability to subvert any security controls of the infrastructure that would negatively impact the business operations.

e. Maintaining contacts with law enforcement authorities, fire department, emergency services and telecommunication providers.

f. Maintaining appropriate contact with special interest groups and authorised information security forums for receiving and distributing the updates on vulnerabilities, security threats, regulations and/ or risks pertaining to the passive infrastructure industry and to the services that are provided by BIL.

g. Addressing Information security in project management activities, regardless of the type of the project and function. The same shall be ensured from the project initiation till and after the project has been rolled out.
4. Mobile device and Teleworking policy

As a part of mobile device policy the user must ensure the below listed requirements:

a. Employees shall be allowed to remotely connect to the BIL network using mobile device to access the business information, only after successful identification and authentication.

b. Employees are required to take special care of the mobile devices such as, but not limited to, laptops, mobile phones, handheld computing devices like PDA etc. that are issued by BIL, to prevent any compromise and/ or destruction of business information.

c. Latest virus definitions shall be regularly updated on the laptops to prevent the corruption of information stored on these devices.

d. Personal firewall shall be installed on the laptops of employees with appropriate policy configured on it.

e. Third party staff shall not connect their computing devices to the network of BIL, unless authorised.

f. Regular awareness sessions shall be conducted for the employees, using mobile computing, to increase their awareness on the additional risks resulting from this way of working and precaution that needs to be taken while using the device.

Below are the listed mobile devices security guidelines in case of handling mobile devices:

a. If the mobile device accesses the Infratel IT applications containing confidential information, access shall be provided via the user authentication (e.g., user ID and password);

b. Mobile devices are easy to spot and are prime targets for theft. It shall be the employee's responsibility to ensure every effort at their disposal is taken to protect the BIL mobile devices, whether in the office or when travelling;

c. If a mobile device is stolen, the local police officials shall be notified. A copy of police report will be obtained, and provided to BIL;

d. Employees are required to have management approval to connect any mobile device (other than Company owned computers) to the BIL network;

e. Any use of Public and/ or Private wireless networks, when accessed with an BIL device, shall be one in accordance with local laws; and

f. No BIL equipment shall be connected to non-BIL networks without appropriate security controls such as personal firewalls and anti-virus software’s.

Teleworking uses communications technology to enable personnel to work remotely from any location outside of their organization. Adequate teleworking security measures shall be established and implemented.
At a minimum the following shall be considered:-

a. Establishing a secure communication channel between the teleworkers and the networks of BIL;

b. Use of appropriate authentication mechanism for authenticating those using the teleworking solutions; and

c. Revocation of authority, access rights and return of equipment when the teleworking activity ceases or when the employee exits from BIL.

As a part of security requirements the users shall consider below listed requirements:

a. Employees are required to take special care of the computing resources used outside the organization such as, but not to, laptops, mobile phones, handheld computing devices like PDA, blackberry, etc. that are issued by BIL, to prevent any compromise and/ or destruction of business information.

b. Users shall be educated, on the use of computing devices in public places, meeting rooms and other unprotected areas outside of the organization's premises.

c. Backups shall be taken at by respective personnel by uploading their critical data on the shared drive.

d. Training shall be arranged for personnel using computing devices outside the organization to raise their awareness on the additional risks resulting from this way of working.

e. BIL shall ensure that security controls are deployed to protect the BIL information, accessible outside BIL’s environment/ premises.

5. Human resource security policy

Background screening, as required for the role, on permanent staff shall be carried out at the time of job applications. A similar screening process shall be carried out or incorporated as part of the contract for contractors and temporary staff in accordance with the risk assessment of the external parties.

Information systems technical details, such as network addresses, network diagrams, and security software employed, shall not be revealed to job applicants until they have been hired and have signed a confidentiality agreement. Persons who have a criminal conviction shall not be hired into, retained for, promoted into, or maintained in computer-related positions of trust. The terms and conditions of employment shall include the employee’s responsibilities for information security and business continuity as laid down by the BIISBCP.

All employees of the organisation and, where relevant, third-party users shall receive appropriate training and regular updates of organisations ISBC MS policies and procedures.
The violation or organisation security policies and procedures by employees shall be dealt through a disciplinary action. The disciplinary action shall be in accordance with the Code of Conduct for BIL and any non-adherence shall trigger Consequence Management Procedure.

The HR function is required to ensure that termination/change of employment responsibilities of the employees, associates and strategic partners are clearly defined, assigned and communicated to them. The HR function is required to formalise a termination process which shall include return of assets that are the property of BIL.

6. Asset Management

Information assets at the BIL shall be classified and based on the impact on the organization, due to loss of their confidentiality, integrity and availability. An inventory of all sensitive (i.e. confidential, restricted) information assets shall be drawn up and maintained to ensure appropriate protection of BIL assets containing information. The asset inventory shall include all information necessary in order to recover from a disaster, including type of asset, backup information, license information, security classification and business value. An owner shall be identified for each of the information assets at the BIL. The owner shall be responsible for:

All employees shall have a personal responsibility for safeguarding all proprietary information, which includes but is not restricted to sensitive documents and information, from disclosure to unauthorized parties.

It is essential to handover the return of all issued assets such as software, corporate documents, equipment, mobile computing devices, mobile phones, access cards, manual and/ or any other asset that is the property of BIL at a time of termination, change of employment responsibilities. Employees shall also be mandated to get sign off from the following department on the no dues form after the return of assets:

a. IT (Technology Services)
b. Human Resources / Admin
c. Finance

Assets containing information useful to the organization shall be classified based on their relative business value, legal requirements and impact due to loss of confidentiality, availability and integrity of the information asset.

a. The level of security shall be identified based on the information classification performed.
b. Assets shall be grouped under the following asset types:

- Physical
- People
• Paper
• Software
• Information

c. Site shall also be considered to be a critical asset supported by the utility services.

d. The information assets shall be classified in the following four categories:

  - **Restricted**: The amount of Company Restricted information is very limited, and is only handled by very few people i.e. authorized personnel only. If unauthorized people gain access to Company Restricted information, this may lead to critical financial, reputational or other damage. Information that is highly sensitive may be available only to specific named individuals (or specific positions).

  - **Confidential**: Information that can be shared amongst a few group of personnel only e.g. specific team, only managers and above etc. If unauthorized people gain access to Company confidential information, this may lead to significant financial, reputational or other damage. Information that is sensitive within the BIL and may be available only to a specific function, group or role.

  - **Internal**: Information that is sensitive outside the BIL and needs to be protected. Authorized Access to employees, contractors, sub-contractors and agents on a "Need to Know Basis" for Business related Purposes. Information that can be shared within BIL and/or with partners who have signed confidentiality clauses. If unauthorized people gain access to Company internal information, this may lead to some financial, reputational or other damage. Most of the information in BIL falls within this classification level. Any unclassified information created and owned by BIL shall be considered as Internal.

  - **Public**: Public Information (including information deemed public by legislation or through a policy of routine disclosure), available to the Public, all employees, contractors, sub-contractors and agents. This type information will not result in any damage if it becomes generally known. There are no limitations on public information regarding creation, distribution, storing, disposal etc.

The owner or creator of information shall assign an appropriate label (Restricted, Confidential, Internal and Public, as above) to the information, and the user or recipient of this information shall consistently maintain an assigned label.

As a part of media handling, BIL discourages the use of removable media for employees and associates. By default, the organization policies should restrict the use of USB and CD/DVD Drives on
their issued laptops and desktops. Policies shall be in place to enforce data read but restrict data write on such devices. In case, media access is required as a part of business process and stated necessary, respective SOD (security override) shall be issued for the purpose. It is recommended for the employees and associates not to store any sensitive (i.e. confidential or restricted) information with non-sensitive information on any removable data storage media unless authorized by the information owner.

Computer media shall be disposed of securely and safely when no longer required. All BIL data on computer rewritable media (such as hard disks) shall be deleted and the media degaussed before disposal. When disposed of, all sensitive information in hardcopy form must be either shredded or incinerated as appropriate. Documents and removable media carrying information of Restricted or Confidential classification shall be transported using only the services of an authorized courier agency and it shall be ensured that the third parties such as, courier agency involved in the transfer signs an agreement ensuring required security of the assets. Such agencies may be subject to an information security audit.

7. Access Control
The Access Control Policy defines the controls that need to be implemented and maintained to protect information assets against unauthorised access that possess substantial risk to the organisation. The policy intends to establish adequate controls for user access management, networks access, operating system security and mobile computing in BIL.

Access to sensitive information shall be granted only when a legitimate business need has been demonstrated and access has been approved in advance by the information owner. Users shall be responsible for all activity that takes place with their user ID and password or other authentication mechanism. A user shall change their password immediately if they suspect that it has been discovered or used by another person and report this to the Central Service Desk.

BIL shall ensure that access to its information and assets is controlled in line with the business and security requirements. Employees and associates shall not use BIL information systems to engage in hacking activities that include, but are not limited to, gaining unauthorized access to any other information systems damaging, altering, or disrupting the operations of any other information systems and capturing or otherwise obtaining passwords, encryption keys, or any other access control mechanism that could permit unauthorized access. Users shall not move information classified at a certain sensitivity level to a less sensitive level unless this action is a formal part of an approved declassification process.

All user IDs on BIL computers and networks shall be constructed according to the BIL’s standard user ID construction, must clearly indicate the responsible individual’s name, and under no circumstances
are such user IDs shall be permitted to be generic, descriptive of an organisational title or role, descriptive of a project, or anonymous. Every user shall have a single unique user ID and a personal secret password for access to the BIL multi-user computers and computer networks. There shall be a formal user access creation and deletion procedure for granting access to all multi-user information systems and services. User creation / modification request shall be initiated by user and is required to be authorized as per predefined delegation of authority. A formal user access provisioning process shall be implemented to assign or revoke access rights for user types to all systems and services.

Creation and allocation of privileged user accounts/ IDs on the information systems shall be controlled through a formal authorisation process. The employee / third party basis the requirement initiates the request for privilege access which undergoes an approval process (basis delegation of authority) for ID Creation. The privileges granted are basis the least requirements and subject to approval from Head IT Security and Head IT Operations. In case there is a change in job role or responsibilities of privilege user, it is the responsibility of the user to update the IT Teams to revoke the accesses. Besides this, as a part of ID validation process all ID’s (including privilege accesses) shall be subject to validation in at least once in 3 months duration. In such a case, the mail notification is sent to the privilege user’s respective manager to ensure if the user has left the system or there is a change in job role. It is the responsibility of the privilege user’s manager to inform the IT Team on the current state of the user and actions shall be taken as advised. Privileges may also be given basis SOD Process i.e. Security Override process.

All BIL systems maximum password age shall be configured to 45 days. This is under the discretion of user to change the same within or on 45th day, post which the password will automatically expire. Users shall not be allowed to use last 5 passwords. All BIL computer systems shall be configured to permit only five attempts to enter a correct password within 24 hours, after which the user ID is locked out and can be reset by the IT Help Desk after authenticating the user's identity or via. IT provided service tool.

The system access history and user logs shall be reviewed periodically by the IT department. Redundant and unused user accounts shall be removed on a periodic basis with at least once in 3 months period. All accounts which are not used for a period of 60 days to be informed to the reporting managers and in scenario of no response to be disabled as per Dormant ID process. The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.
8. Cryptography

The cryptography policy defines the security standards and requirements associated with the use of cryptographic services within BIL. It is intended to define the required protection level to maintain the confidentiality, integrity and authenticity of the confidential information assets and sensitive application systems of BIL.

BIL shall support the encryption algorithms suitable for its business needs. Use of a particular encryption algorithm to ensure privacy and integrity of information shall be decided by the IT function in consultation with CISO.

9. Physical & Environmental Security

The administration function is required to define the physical security perimeter for all office locations, facilities and the geographies where information assets of BIL are located. Physical access restrictions commensurate with the criticality value of information assets shall be implemented at perimeter of all such facilities, where these are hosted.

Access to every office, computer room, and work area containing sensitive information shall be physically restricted to limit access to authorized personnel only. All persons (including employees, visitors, partners etc.) shall wear an identification badge on their outer garments ensuring that both the picture, in case of employees; and information on the badge are clearly visible whenever they are in BIL secure buildings or facilities. Employees shall not permit unknown or unauthorized persons to pass through doors, gates, and other entrances to restricted areas at the same time when they go through these entrances. Visitor or other third-party access to BIL offices, computer facilities, and other work areas containing sensitive information shall be controlled by guards, receptionists, or other staff.

All facilities shall remain secured during and after office hours or when unattended. Appropriate level of security controls shall be implemented to prevent unauthorised access in office areas and facilities hosting critical equipment. Multi-user computer and communications facilities (including telephone closets, network router and hub rooms, voice mail system rooms, and similar areas containing computer and / or communications equipment) shall be kept locked at all times and not accessed by visitors without an authorized IT staff escort to monitor all work being performed. The areas where critical information systems or equipment are located are defined as Restricted (Secure) Areas. Such areas include the Data Centres, Tower Operation Centres, etc. The administration function with the assistance of IT function are required to identify all restricted areas and implement additional security controls to prevent intrusion and damage to these areas.
It shall be ensured that all areas, where loading and unloading of items are done, are monitored and equipped with the appropriate physical security controls during these activities. Access to these areas shall be confined to authorized personnel only during these activities. The movement of all incoming and outgoing items shall be documented and incoming items shall be inspected for potential threats.

Equipment security controls shall be implemented to prevent loss, damage, theft or compromise of information systems and interruption to the organization’s activities. Employees shall not bring their own computers, computer peripherals, or computer software into BIL facilities without prior authorization from their department head / IT Department.

Employees, associates and strategic partner party staff are required to ensure that information systems of BIL are disposed of only after obtaining approval from authorized personnel. Sensitive information and licensed software shall be removed from the media prior to its disposal. Equipment shall be disposed in an environmentally sensitive manner, taking account of any recycling facilities provided by manufacturers, local authorities or commercial organizations. All employees with access to information assets shall be made aware of the information security requirements and procedures for protecting unattended equipment. Equipment, information or software belonging to the organization shall not be removed without authorization of the relevant functional head or asset owner.

BIL shall have a clear desk and a clear screen policy aimed at reducing the risks of unauthorized access, loss of, and damage to information.

10. Operations Security
All production computer and communications systems at the BIL shall employ a formal change management procedure to authorize all significant changes to software, hardware, communications networks, and related procedures. Changes to all information processing facilities and systems shall be controlled and documented to ensure that any changes and additions do not compromise information security.

The use of computer and network resources shall be monitored, tuned, and projections shall be made for future capacity requirements to ensure the required system performance and to avoid misuse and excessive use of resources.

Employees and associates shall not establish intranet servers, electronic bulletin boards, local area networks, modem connections to existing internal networks, or other multi-user systems for communicating information without the prior approval of Head IT Security.
Separate people shall perform production application source code development and maintenance, production application staging and operation, and production application data manipulation.

BIL identifies detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness. Malicious software (malware) checking systems shall run continuously on all personal computers, local area network servers, firewalls, and on electronic mail servers. All files coming from external sources shall be checked before execution or usage. If users obtain malicious software alerts, they shall immediately disconnect from all networks and cease further use of the affected computer, and call the IT Helpdesk for technical assistance and shall make no attempt to eradicate the virus.

Regular backups shall be taken for all essential business information; a backup plan shall be documented identifying the information systems, information to be backed up, type and frequency of backups. All back up activities shall be logged through an event trail. Every user shall back up the local data on their workstations and laptops on the network drive/ shared folder as appropriate.

All production application systems that handle sensitive BIL information shall generate logs that capture every addition, modification, and deletion to such sensitive information.

Access to installed software on production systems shall be restricted to the authorised personnel only. Software requirements for any department shall have an appropriate business case and budget approvals from the business department and shall obtain a technical clearance from the IT department before deployment in the production system.

IT department shall be exclusively responsible for installing and supporting software on BIL computers for:

a. Office desktop computers (Local and Remote Locations);
b. BIL computers systems (Local and Remote Locations); and
c. Servers (Local and Remote Locations).

11. Communications Security

BIL shall ensure adequate management and control of networks to protect information in systems and applications. The network controls shall include, segregation of networks as per zoning architecture for secure areas, protection of critical information systems through a firewall, network documentations such as updated network diagrams etc. Appropriate controls shall be put in place to protect the IT infrastructure against unauthorized access, modification and/ or destruction.
All inquiries made by external agencies or personnel shall be diverted to the designated spokespersons. All employees shall take all possible care to avoid information disclosure while discussing BIL information in public places such as in building lobbies or on public transportation.

All employees who shall be delivering speeches, writing papers, or otherwise disclosing information about the BIL or its business shall obtain pre-authorization from CSMO, which is then forwarded to Bharti Corporate Communications department.

Exchanges of in-house software or internal information between the BIL and any third party shall be accompanied by an agreement that specifies the terms of the exchange, and the manner in which the software or information is to be handled and protected.

Before employees release any Sensitive BIL information, or enter into any contracts, the identity of the individuals and organizations contacted shall be confirmed through digital certificates, letters of credit, third-party references, or telephone conversations.

BIL system administrators shall maintain electronic mail messages and including logs as per backup management procedure. Employees shall not employ any electronic mail addresses other than official BIL electronic mail addresses for all BIL business matters. Unless the Information Owner or originator agrees in advance, or unless the information is clearly public in nature, employees shall not forward electronic mail to any address outside of the BIL network.

a. Employees and associates shall not create and send, or forward externally-provided electronic mail messages that may be considered to be harassment or that may contribute to a hostile work environment.

b. An electronic mail message shall be retained for future reference if it contains information relevant to the completion of a business transaction, contains potentially important reference information, or has value as evidence of BIL management decision.

c. Employees and associates shall not send or forward any messages through BIL information systems that may be considered defamatory, harassing, or explicitly sexual, or would likely offend someone on the basis of race, gender, national origin, sexual orientation, religion, political beliefs, or disability.

d. Employees and associates shall not use BIL computer systems for the transmission of any type of unsolicited bulk electronic mail advertisements or commercial messages that are likely to trigger complaints from the recipients.

e. Users who receive an unexpected attachment to an electronic mail message that does not have a credible business-related explanation shall not open the attachment until they obtain an explanation from the sender.

Confidentiality or non-disclosure agreements shall address the requirement to protect confidential information using legally enforceable terms. Confidentiality or non-disclosure agreements shall be applicable to external parties and employees of the organization.
Requirements for confidentiality or non-disclosure agreements reflecting BIL needs for the protection of information shall be identified and maintained and this shall be based on the criticality of the information to be protected. These requirements shall be reviewed as per the contract terms and/or at the time of any change of the business environment, legal requirements and contractual obligations.

12. System acquisition, development and maintenance
Before a new system is developed or acquired, management of the user department along with IT shall clearly specify the relevant security requirements. Business requirements for new systems or enhancements to existing systems shall specify the required security controls.

All software developed in-house to process sensitive, valuable, or critical information such as production systems, shall have a written formal specification that is part of an agreement between the involved information owner and the system developer, and drafted and approved.

All software developed in-house that runs on production systems shall be developed according to the Software Development Lifecycle (SDLC) or any other agreed software development methodology in agreement with IT. As a part of development the software shall be adequately documented and tested before it is used for critical BIL information. Information systems and applications that are accessed from the external networks and Internet shall be equipped with session time out, connection time slot and appropriate encryption to ensure the confidentiality, integrity and availability of the information is maintained.

For the customised (not off-the-shelf/ standard offerings) software developed by strategic partners/third parties, arrangements pertaining to licensing, code ownership and intellectual property rights shall be documented in the contract between BIL and the strategic partner/third party. The contract shall include that BIL reserves the right to audit quality and accuracy of software development and testing. Such software code shall have escrow arrangements as appropriate.

13. Supplier Relationships
Legal and Supply Chain functions shall identify and mandate information security controls to specifically address third party/ vendor/ supplier access to BIL information.

BIL shall provide compliance requirements (where applicable) in the agreements with third parties involving accessing, processing, communicating or managing BIL information or information processing facilities shall cover all relevant security requirements. Non-Disclosure Agreements or Confidentiality clauses within the agreement shall be defined to ensure information security.

Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology supply chain:
a. Defining information security requirements to apply to information technology service acquisition in addition to the general information security requirements for supplier relationships;

b. For information and communication technology services, requiring that suppliers propagate BIL security requirements throughout the supply chain if suppliers subcontract for parts of information service provided;

c. Implementing a monitoring process and acceptable methods for validating that delivered information services are adhering to stated security requirements;

d. Obtaining assurance that critical components and their origin can be traced throughout the supply chain;

e. Obtaining assurance that the delivered information and communication technology services are functioning as expected; and

f. Sharing of information regarding the supply chain and any potential issues and compromises among the organization and suppliers.

BIL emphasizes the need on effective governance on the supplier services. Service reports and evidences from third parties / suppliers shall be reviewed at regular intervals as per the contract or agreement with business.

Audits may be conducted at specified intervals to assess the compliance of third parties with the agreed contracts and the clauses of non-disclosure and confidentiality incorporated in the contracts. Review of third party audit trails and records of security incidents, operational problems, failures, fault logging and disruptions shall be done as per the pre-defined frequency. Identified problems/ issues shall be managed and resolved with the supplier/ third party.

14. Information security incident management

Management shall establish a procedure to ensure an effective, timely and orderly response to information security incidents. Guidelines shall be established for collective and maintaining evidences collected as required by legislation.

BIL shall establish a framework for reporting, responding to, and escalating information security and business continuity events and configure the same in the incident management system or as appropriate. All employees, contractors and third party users shall be responsible for reporting all identified security events and incidents promptly.

BIL shall establish an incident management procedure for reporting, responding to, and escalating any suspected security weakness or threat to systems or services. Users shall report all information security alerts, warnings and suspected vulnerabilities to the management, in a timely manner, and shall share such information with only with authorized personnel. Employees shall promptly notify management of all conditions that could lead to a disruption of business activities.
Reported incidents shall be assessed to verify if these shall be reported as security incidents. Classification and prioritization of an incident shall help to identify the impact and extent of an incident. Incident assessment shall be carried out by the Damage Assessment Team and the same shall be submitted to Crisis Management Team (as appropriate). All information security incidents shall be responded as per an incident management procedure or as directed by management.

Information security incidents shall be monitored and analysed on time to time basis. Incidents with high business impact shall be identified and appropriate controls shall be enhanced to reduce the risk from future occurrences of such incidents. The learning’s from the same are shared with the respective teams along with corrective actions taken.

Where action against a person or organization involves the law, either civil or criminal, the evidence collection and presentation shall conform to applicable laws. This shall include compliance with any published standard or code of practice for the production of admissible evidence.

All Investigations of alleged criminal or abusive conduct shall be treated as restricted information to preserve the reputation of the suspected party until charges are formalized or disciplinary action taken. All internal investigations of information security incidents, violations, and problems, shall be conducted by staff authorized.

15. Information Security aspects of business continuity

BIL shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster. Information security aspects of business continuity shall be identified and documented in the business continuity framework as appropriate.

Functional heads shall be responsible for ensuring that the key events that can cause disruption to their processes are identified and their potential adverse impact is documented. The following shall be considered while implementing any business continuity program:

- a. identify critical business functions, applications and supporting technologies;
- b. develop an appropriate cost effective recovery strategy;
- c. identify and document the required recovery actions, identify and ensure the availability of required resources, and compile this information as the recovery plan;
- d. train the recovery teams in the activities of their specific tasks;
- e. identify vendor recovery support capability;
- f. identify functional team, recovery support and response capabilities; and
- g. Develop an ongoing testing and maintenance program to ensure that all processes are in a constant state of recovery readiness.
BIL shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.

All departments shall establish and use a logical framework for classifying all information resources by recovery priority that shall permit the most critical information resources to be recovered first. All functions shall prepare, periodically update and regularly test the business recovery plan that specifies how alternative facilities shall be provided so employees can continue operations in the event of a business interruption.

BIL shall develop continuity plans which shall be exercised, tested and integrated into the organizations business processes. These continuity plans shall be routinely tested and followed up with a brief report to top management detailing the results. The roles and responsibilities for business continuity planning shall be reviewed and updated annually.

The respective departments shall identify business requirements for the availability of information systems and its processing facilities. Alternate sites shall be determined to carry out critical business processes with respective arrangements or as appropriate.

16. Compliance
All relevant statutory, regulatory and contractual requirements shall be defined and documented for all information processing facilities. The legal function shall track the compliances from respective functions; whereas it is the responsibility of each function to ensure the compliance and submit the reports to legal.

BIL shall be the legal owner of all business information stored on or passing through its systems, except the information clearly owned by third parties. All intellectual property, such as patents, copyrights, inventions, etc., developed by a user while employed by BIL, shall be the property of BIL. At the time of termination of their relationship with the BIL, all employees shall return any intellectual property provided or developed during the period of the person's employment. All BIL intellectual property shall be classified as per the BIL’s information classification guidelines available in asset management policy and labelled and handled as per BIL policies.

BIL shall manage the lifecycle of all records created or received by it in pursuance of legal obligations or transactions of business. All records and information, such as personnel details, legal documents, shall be retained and disposed only in accordance with the retention periods as per the applicable laws. All sensitive information shall be destroyed in secure manner.
BIL shall implement controls for collecting, processing, and disseminating personal information. Employee personal data maintained on information systems shall be secured through implementation of appropriate security controls. Only select authorized personnel shall have access to such information or as per the segregation of duties matrix submitted by the CBT members of respective function.

The security controls shall address:

- Mechanisms for ensuring that information is obtained and processed fairly, lawfully and properly.
- Ensuring that information is accurate, complete and up-to-date, adequate and relevant.
- Appropriate weeding and deletion of information.
- Compliance with individual’s rights, such as subject access.
- Compliance with the relevant data protection/ privacy regulations.

BIL may log, review, and utilize any personal information stored on or passing through its systems. The organization shall, at its discretion, monitor usage of its information assets as per applicable laws and terms and condition of employment agreed upon by the BIL and the employee. This may include logging and reviewing of user activity such as telephone numbers dialled, web sites visited from BIL owned assets, electronic communications exchanged through BIL information processing facilities etc. BIL top management shall initiate an independent review of the information security and business continuity. Such an independent review is necessary to ensure the continuing suitability, adequacy and effectiveness of the organization’s approach to managing ISBC.

Respective Departmental Heads and/or CG Members shall ensure compliance with this information security policies and other respective policies. The CISO is authorized to perform compliance checks against security policy. The frequency of such compliance checks shall be performed according to the size of the facility or prior audit results, and if any non-compliance is found as a result of the review, management shall:

a. Determine the causes of the non-compliance;

b. Evaluate the need for actions to avoid recurrence of the same;

c. Determine and implement appropriate corrective action; and

d. Review the corrective action taken

Results of reviews and corrective actions carried out shall be recorded and these records shall be maintained. Managers shall ensure adherence to information security requirements in their teams and within their area of responsibility.
Management shall ensure review of information systems for issues basis the approved scope by the board. As a part of the management direction ITGC audits and application reviews shall be conducted at least annually. These reviews shall ensure the compliance of information systems to the prescribed policies in place. The responsibility of driving the closure of the observations lies with the respective function whereas the Internal Controls team shall ensure overall governance towards closure of identified gaps. The technical compliance checks shall also be carried out as a part of operations. The technical compliance checks shall also be carried out as a part of operations.

I. Document Distribution

The Chief Information Security Officer (CISO) shall distribute this document to Bharti Infratel employees and associates as per the requirement.

II. Document Conventions

The statements containing the words ‘shall’ and ‘required to’ in the document are mandatory requirements. Failure to observe these requirements may be construed as non-compliance to the policy.

The statements containing the word ‘recommended’ imply a desirable requirement. Failure to adhere to these requirements may not be a direct non-compliance.