bharti | REAL ESTATE

INFORMATION SECURITY POLICY

VERSION – 2.6/2023

DATE OF ISSUE – 12th JULY 2017

Kumar

APURV KUMAR
HEAD INFORMATION TECHNOLOGY
DOCUMENT OWNER

S K SAYAL
MANAGING DIRECTOR & CEO
APPROVED BY

Document Control

S. No.	Type of Information	Document Data
1.	Document Title	Bharti Real Estate Information Security Policy
2.	Document Code	BRISP/Realty
3.	Date of Release	12/10/2023
4.	Document Superseded	
5.	Document Revision No	Version 2.6
6.	Document Owner	Apurv Kumar- VP Finance and IT
7.	Document Author(s)	Deepak Sharma – Manager IT

Document Approvers

S. No.	Approver	Approved Through / Nominee(s)	Nominee(s) Contact
1.	Apurv Kumar		
2.	Deepak Sharma		
3.			

Document Change Approvals

Version No.	Revision Date	Nature of Change	Date Approved
2.0	12/07/2017	Process Alignment	
2.1	31/12/2017	Process Alignment	31/12/2017
2.2	29/11/2018	Process Alignment	3/12/2018
2.3	30/01/2020	Process Alignment	07/02/2020
2.4	22/07/2020	Process Alignment	12/08/2020
2.5	30/09/2022	Process Alignment	12/10/2022
2.6	30/09/2023	Process Alignment	12/10/2023

I) Document Distribution

The IT Head shall distribute this document to all document change reviewers when it is first created and as and when changes or updates are made. The IT Head shall distribute the document to all members of the Information Security Steering Committee (ISSC) and the Information Security Working Group (ISWG).

The IT Head is responsible for communicating the latest version of Bharti Real Estate Information Security Policy (BRISP) to all the functions.

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.

III) Document Organisation

This document is organised under the following sections: -

- Information Security Policy
- Information Security Policy Framework

Index

1. Information Security Policy

1.1. Introduction

It is the policy of Bharti Real Estate that its information assets are provided with possible protection against the external threats and interruptions in the business service availability.

The Bharti Real Estate Information Security Policy (hereinafter referred to as BRISP in this document) provides management direction and support to implement information security across Bharti Real Estate.

1.1.1 Scope

The BRISP is applicable to all information assets of Bharti Real Estate. An information asset is a definable piece of information, stored and/ or processed in any manner, which is recognised as valuable to the business. The types of Information assets could be software assets, physical assets, paper assets, services assets, people assets and information assets that are physically or electronically stored, processed and/or transmitted by any of the aforesaid types of assets.

The BRISP is applicable to all employees and third parties of Bharti Real Estate.

As a reference for this document, a service provider is called a Third-party only after association with Bharti Real Estate. These third parties are strategic partners who enter into direct contracts with Bharti Real Estate 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 partners are required to provide to Bharti Real Estate. Third parties include IT service providers, telecommunication service providers, value added service providers (VAS, VAS O&M), sub-contractors and other consultants/ representatives of the above mentioned third parties.

The term ‘third party staff’ mentioned in this document refers to the employees, agents, consultants and representatives, of all third parties, who are in any way accessing, processing, storing or transmitting any information assets of Bharti Real Estate.

The BRISP is applicable across all business units of Bharti Real Estate. The BRISP is applicable across all geographies where the information assets of Bharti Real Estate are located.

1.1.2 Policy Owner

The owner of the BRISP is the Head of Information Technology (hereinafter refer as IT Head in this document). The IT Head shall be responsible for the maintenance and updating of the BRISP document.

1.1.3 Responsibility

Information Security Steering Committee (ISSC): The ISSC, as defined in the *section 2.3.1* of this document, shall be responsible for approving the BRISP and any subsequent modifications to the BRISP.

Head of Information Technology (IT Head): The IT Head, as defined in the *section 2.3.2* of this document, shall be responsible for ensuring that policies constituting the BRISP are current and reflect the requirements of Bharti Real Estate.

1.2. Policy Statement and Objective

Security of information assets of Bharti Real Estate is of paramount importance and confidentiality, integrity and availability of these shall be maintained at all times through controls commensurate with the asset value.

The BRISP provides management directive for information security and recommends appropriate security controls that need to be implemented to maintain and manage the information security in Bharti Real Estate. Bharti Real Estate shall strive to secure information by: -

a. Establishing and organising an Information Security Governance Framework.

b. Developing and maintaining an effective Information Security.

c. Deploying appropriate technology, resources, and infrastructure.

d. Constantly monitoring, reviewing, exception-reporting, and taking actions thereon for improving the effectiveness.

e. Taking appropriate actions for any violations of the BRISP.

1.3. Review and Evaluation

The BRISP document shall be reviewed at the time of any major change(s) in the existing environment affecting policies and procedures or once every year, whichever is earlier. The BRISP document shall be reviewed by the IT Head and approved by the ISSC. The reviews shall be carried out for assessing the following: -

a. Impact on the risk profile due to, but not limited to, the changes in information assets, deployed technology/ architecture, regulatory and/ or legal requirements; and

b. The effectiveness of the policies.

As a result of the reviews, additional policies could be issued and/ or existing policies could be updated, as required. These additions and modifications would be incorporated into the BRISP document. Policies that are identified to be redundant shall be withdrawn.

1.4. Consequence Management for Non-Compliance

a. All employees and third parties are required to comply with the BRISP.

b. Non-compliance with the BRISP is ground for consequence (COC), up to and including termination. The relevant HR process shall be invoked for further persuasion.

c. If it is ascertained that the action is inadvertent or accidental, first violation(s) shall result in a warning. A relevant warning letter shall be placed in the involved person's personal file. Subsequent violations could result in dismissal.

1.5. Exceptions

The BRISP is intended to be a statement of information security requirements that need to be met in Bharti Real Estate. However, exceptions against individual controls in specific policy domains shall be formally documented which will include the following: -

a. Justification for the exception.

b. The validity period of the exception.

c. Approval from the authorities.

2. Information Security Organisation Policy

2.1. Introduction

The *Information Security Organisation Policy* defines appropriate responsibilities, authority and relationships to manage information security. The information security organisation has representation from required business functions to ensure the structured co-ordination of information security related activities.

2.1.1 Responsibility

It is the responsibility of the Information Security Steering Committee (ISSC) and IT Head to manage the information security organisation within Bharti Real Estate.

2.2. Policy Statement and Objective

An information security organisation shall be set up to undertake information security activities.

The objectives of *Information Security Organisation Policy* are to ensure that: -

a. A system is established to implement, monitor, manage and improve organisation-wide information security framework.

b. The security roles and responsibilities are defined and assigned at all levels ensuring that the individuals understand them.

c. All employees and third parties are aware of their information security requirements, and they implement them in letter and spirit.

d. The information risks concerning operational activities, infrastructure and projects are assessed.

e. The risk treatment plans are developed and implemented to mitigate unacceptable information risks; and

f. The ISMS is reviewed at regular intervals and the appropriate actions are taken and implemented enabling the ISMS to achieve the declared objectives.

2.3. Bharti Real Estate Information Security Organisation Structure

2.3.1 Information Security Steering Committee (ISSC)

The ISSC shall provide the management direction and support for the information security initiatives. The ISSC shall comprise the following members: -

a. Chief Finance Officer - Finance

b. Head of Department – Information Technology

The IT Head would be the coordinator of the ISSC.

The ISSC shall have the following responsibilities: -

a. Approving the Bharti Real Estate Information Security Policy.

b. Providing the resources needed for information security and approving assignment of specific roles and responsibilities for information security across the organisation.

c. Communicating the information security plans and programs to maintain information security awareness in Bharti Real Estate.

d. Deciding the acceptable levels of risk and providing the feedback for the improvement.

2.3.2 Head of Information Technology (IT Head)

The IT Head is responsible for the establishment and maintenance & shall have the following responsibilities: -

a. Identifying information security objectives and strategizing them consistently.

b. Managing the development and implementation of the BRISP and its procedures to ensure ongoing maintenance of information security.

c. Overseeing operations, including information incident management and business continuity management.

d. Overseeing investigations/forensics of security breaches, including suspected insider threat.

e. The IT Head could issue ‘special instructions’ in emergent cases required for carrying out investigations and forensics. Such special instructions would be issued by the IT Head to the investigation team to enable maintaining confidentiality of the investigation and achieving speed in collecting evidentiary material before the same is either destroyed or altered knowingly or wilfully by those being investigated.

f. Assisting in consequence management and legal matters associated with such breaches, as necessary.

g. Managing the development and implementation of information security training and awareness programmes; and

h. Keeping the management updated with effective, efficient and reliable approaches for information security.

2.4. Contact with Authorities

Contacts with law enforcement authorities, fire department, emergency services and shall be maintained by the Administration function. The contact details of these agencies should be maintained and displayed at appropriate places that are accessible to users.

2.5. Third-party Security

a. All third parties are required to adhere to the *Bharti Real Estate Information Security Policy (BRISP)*. If the third parties' sub-contract any service/work pertaining to Bharti Real Estate, the sub-contracted parties and their employees are also required to adhere to the policy.

b. All Third-parties are required to submit either Code of conduct, Non-disclosure documents or should submit the acknowledge copy of agreement which has confidentiality clause with respect to information security.

c. In accordance with the BRISP, Third-parties shall be subject to independent reviews of their compliance with the BRISP.

2.5.1 Identification of Risk Related to Third-party Access

The IT function required to carry out a risk assessment to identify the information security implications and the asset owner has to mitigate/avoid/accept risk as per risk assessment methodology defined by Bharti Real Estate.. The asset owner is responsible for accepting the risk related to third party access to their information assets before access to information asset is provided to a third party. Based on the results of the risk assessment, appropriate access controls shall be designed and implemented prior to providing access to the third party. The following shall be considered to design the access controls: -

a. Maintaining the security of information assets that are accessed or managed by the third party.

b. Allowing connectivity in a secure manner between Bharti Real Estate and the third party only for what is explicitly required for information exchange. Everything else shall be denied; and

c. Clearance from the IT Head office is obtained before providing any access to third parties.

3. Asset Management Policy

3.1. Introduction

The *Asset Management Policy* specifies the importance of information assets including identification of the asset owner, asset classification and determining confidentiality, integrity, and availability. The policy establishes the requirement of controls that need to be implemented for protecting information assets.

3.1.1 Responsibility

It is the responsibility of the Head of Department (HOD) of each function that owners are identified for all the information assets belonging to his/ her function and ownership is assigned to them.

The asset owners are responsible for identifying, classifying, and ensuring the protection of their respective information assets with the help of Information Technology. The asset owner is also responsible for identifying the asset custodians for the assets under his/ her ownership and extend the information access with the Help of Information Technology.

The asset custodians are responsible for the implementation of the required controls (Access control over the Document vault) for the protection of information assets.

3.2. Policy Statement and Objective

Information assets of Bharti Real Estate shall receive comprehensive protection and shall have an identified owner.

The objectives of the policy are to ensure that: -

a. An information document vault containing all types of information assets of each business function is maintained.

b. The information assets of each business function have designated owners and custodians; and

c. Access control over the information assets.

3.3. Responsibility of Asset Management

The asset owner is accountable for the comprehensive protection of information assets owned by him/her. The asset owner may delegate the responsibility of applying the relevant controls for the maintenance of the assets to an individual/ function referred to as the ‘asset custodian’. It is the responsibility of the asset custodian to implement appropriate security controls that are required for the protection of information assets. It is the responsibility of all employees and third-party staff to maintain the confidentiality, integrity and availability of the information assets that they use.

3.3.1 Ownership of Assets

The head of each business function is required to ensure that his/ her function's information assets have identified along with their owners. The asset owners shall be responsible for the appropriate classification of the asset and shall ensure that the security controls required to protect the assets are implemented.

3.4. Information Classification

The information has different degrees of sensitivity and criticality to the business. The information classification categories shall be used to define an appropriate level of protection or special handling. The classification of the information needs to be consistent as per the business requirement.

Employees and third-party staff are required to classify the information that they create for Bharti Real Estate as per the following classifications: -

a. Confidential

This classification applies to any sensitive business information which is intended for use within Bharti Real Estate. Its unauthorised disclosure could adversely impact its business, its shareholders, its business partners, its employees and/or its customers.

b. Internal

This classification applies to information that is specifically meant for employees of Bharti Real Estate. While its unauthorised disclosure is against the policy, it is not expected to seriously or adversely impact the business, employees, customers, stockholders and/ or business partners.

Any information provided by the Bharti Real Estate to the Service Provider which was not available in the public domain including the terms and conditions of the Agreements, shall be treated as Confidential Information, and shall not be disclosed by the Service Provider without prior written consent of the Company.

3.4.1 Exception:

a) Information circulation to internal to organization does not necessarily require information classification.

b) The classification of the document is subjective and limited to the information owner's discretion / understanding about the content / information for classification.

4. Human Resources Security Policy

4.1. Introduction

The *Human Resources Security Policy* specifies the information security requirements that need to be integrated in the HR processes including recruitment, employment, and separation.

4.1.1 Responsibility

The IT functions are required to support the HR function for the implementation and maintenance of technology related controls.

4.2. Policy Statement and Objective

Information security controls shall be designed to ensure that employees and third-party staff understand their responsibilities and to reduce the risk of theft, fraud or misuse of information assets.

4.3. During Recruitment

The Human Resources (HR) function shall ensure that security responsibilities are clarified to every new employee when he/she joins the organisation as part of induction program or COC guide.

4.3.1 Roles and Responsibilities

The HR function shall ensure the following: -

a. Shall Inform IT Team well in advance to ensure that the assets required to perform his role should be made available.

b. Shall raise appropriate requests to authorise the new employee to gain access on the Bharti Real Estate network.

4.4 During Employment

4.4.1 Reporting Security Weaknesses and Incidents

a. It is the responsibility of each employee to report any observed or suspected information security incidents and/ or weaknesses to the IT Helpdesk and send an email to MY.IT@bhartirealty.com. Any other action required as per the *Information Security Incident Management Process* shall also be taken.

b. The employees and third-party staff shall not attempt to exploit or prove any suspected security weaknesses. Testing weaknesses could cause damage to the information system or service. Any such attempt would be interpreted as a potential misuse of information system and may result in legal liability for the individual performing such testing.

4.5 Termination or Change of Employment Responsibility

4.5.1 Termination Responsibilities

a. The HR function is required to ensure that termination/ change of employment responsibilities of the employees and third parties are clearly defined, assigned, and communicated to them.

b. The HR function is required to formalise a termination process including the return of all issued assets such as software, corporate documents, equipment, mobile computing devices, credit cards, access cards, manual and/ or any other asset that is the property of Bharti Real Estate.

c. All employees and third-party staff are required to return all information assets that are issued to them.

4.5.2 Removal of Access Rights

a. The HR, IT functions are required to ensure that the access rights of all employees and third-party staff to information assets are revoked upon termination of their employment, contract or agreement.

b. The IT functions are required to ensure that passwords for active accounts of a departing employee or third-party staff are changed immediately on the departure of the employee.

c. The IT functions are required to ensure that, in case of any change (including exit) in the responsibilities of an employee or third-party staff, the access rights are revoked or modified as required.

d. IT team to ensure that domain id and email id should be deactivate with-in 3 working days after HR mail confirmation.

5. Physical and Environmental Security Policy

5.1. Introduction

The *Physical and Environmental Security Policy* provides direction to the Administration Department of Bharti Real Estate for the development and implementation of appropriate security controls that are required to maintain the protection of information systems and processing facilities from physical and environmental threats.

5.1.1 Responsibility

The Administration function is primarily responsible for the implementation & Maintenance (incl. Management & AMC) of controls defined in the *Physical and Environmental Security Policy*.

The IT functions, however, are required to support the Administration function for the implementation of physical and environmental security controls as specified in this policy.

5.2. Policy Statement and Objective

Bharti Real Estate shall provide adequate protection to its information systems and facilities against unauthorised physical access and environmental threats. Appropriate controls shall be implemented to maintain the security and adequacy of the information systems and equipment.

The objectives of the policy are to: -

a. Prevent unauthorised physical access, damage and interference to the organisation's premises and information.

b. Ensure that critical information systems are located in secure areas, protected by the defined security perimeters, with appropriate security barriers and entry controls.

c. Protect the information assets by implementing environmental controls to prevent damage from environmental threats; and

d. Administration department to regularly conduct the preventive maintenance of the utility equipment to ensure their faultless services.

5.3. Physical Security Controls

5.3.1 Perimeter Security

The Administration (Admin Dept. Of Bharti Real Estate) function is required to define the physical security perimeter for all office locations, facilities, and the geographies where information assets of Bharti Real Estate are located. It is recommended that physical access restrictions commensurate with the criticality value of information assets are implemented at perimeter of all such facilities where these are hosted.

5.3.2 Physical Entry Controls

a. Access to offices, facilities, and secure areas (such as Data Centres, Network Operation Centres,) shall be provided to authorised personnel only. Access to secure areas shall be controlled and monitored.

b. Separate log should be created to monitor the activity in the area such as data Center.

5.3.3 Working in Secure Areas

The areas where critical information systems or equipment are located are defined as Secure Areas. Such areas include the Data Centres, Network Operation Centres, Security Operations Centre, etc. The administration function with the assistance of IT functions is required to identify all secure areas and implement additional security controls to prevent intrusion and damage to these areas. The Administration function shall ensure that: -

a. Physical access controls should be implemented in these areas.

b. Personnel are provided access to these areas on need to have basis only.

c. Physical movements in such areas are monitored or recorded as far as possible.

5.4. Environmental Security

Protection against damage from environmental threats shall be designed and implemented. It is recommended to consider the following for designing the environmental protection system: -

a. Air-conditioning systems to support information systems and equipment.

b. Implementation of appropriate fire protection measures, including installation of fire-suppression systems in areas such as Data Centres.

c. Implementation of adequate power supply controls to ensure continuous power supply.

5.5. Equipment Security

Equipment security controls shall be implemented to prevent loss, damage, theft or compromise of information systems and interruption to the organisation’s activities.

5.5.1 Equipment Location and Protection

IT Equipment shall be protected against environmental threats and unauthorised access. IT and Administration functions shall ensure that: -

a. The equipment are appropriately located and security controls are implemented to reduce the risk of potential threats (e.g. theft, fire, smoke, electrical supply interference) for their continued operations;

b. Unattended equipment such as servers, network, wireless and telecom devices are placed in secure enclosures; and

c. Appropriate environmental protection controls are identified and implemented for the safety of the equipment.

5.5.2 Equipment Maintenance

All equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.

IT and Networks functions shall ensure that preventive maintenance for the server and network devices is carried out at regular intervals to protect them from dust and other similar deposits that may impair the functioning of these systems.

For utility equipment, the Administration function shall ensure that: -

a. All supporting utilities, such as electricity, water supply, sewage, heating/ventilation and air conditioning, are in appropriate condition for the information systems and/ or facilities that they are supporting.

b. Uninterruptible power supply (UPS) systems and generators are installed to support controlled shutdown or continued functioning of equipment supporting critical business operations.

c. An alarm system to highlight the malfunctions in the supporting utilities is installed.

d. Adequate contacts are in place with other authorities including utilities, emergency services, health and safety departments.

5.5.3 Secure Disposal

a. Employees and third-party staff are required to ensure that information systems of Bharti Real Estate are disposed/scraped only after obtaining approval from authorised personnel.

b. Disposal/scrapping of IT equipment such a laptop, desktop shall be done by Bharti Real Estate IT Team.

c. Data and licensed software shall be removed from the IT Equipment prior to its disposal.

d. Scrap disposal shall be done with the help of government authorised vendor only.

6. Communication and Operations Management Policy

6.1. Introduction

The *Communication and Operations Management Policy* establishes appropriate controls that need to be implemented to prevent unauthorised access, misuse or failure of the information systems and equipment and to ensure confidentiality, integrity and availability of information that is processed by or stored in the information systems/ equipment.

6.1.1 Responsibility

The IT team is responsible for the implementation of controls defined in this policy in the IT infrastructure.

Administration function is responsible for providing its support to IT functions during the implementation and maintenance of the controls defined in this policy.

6.2. Policy Statement and Objective

Bharti Real Estate shall ensure effective and secure operation of its information systems and computing devices. Appropriate controls shall be implemented to protect the information contained in and/ or processed by these information systems and computing devices.

The objectives of this policy are to: -

a. Ensure protection of information during its transmission through communication networks.

b. Protect the confidentiality, integrity, and availability of information assets from the adverse impact of malicious code.

c. Develop an appropriate backup procedure for ensuring the availability of information and communication services; and

d. Ensure the antivirus signatures are updated with the latest signatures in order to prevent information.

6.3. Operational Procedures and Responsibilities

6.3.1 Documented Operating Procedure

a. A Standard Operating Procedure (SOP) shall be developed as and when a new information system or service is introduced. The SOP shall include the necessary activities to be carried out for the operation and maintenance of the system or service and the actions to be taken in the event of a failure.

b. The procedure shall encompass necessary checklists to implement the various activities mentioned above.

c. A Standard Operating Procedure (hereinafter referred to as the SOP) shall be created to maintain the confidentiality, integrity and availability of the specific platform or application. The procedures shall include, but not limited to, the following: -

   i. Any automated or scheduled processes that are running on the system or application.

   ii. Day-to-day operational tasks that need to be performed by the operator.

   iii. Actions performed when an error or an exception condition occurs, including the listed contact details of people that may be required to assist or that may be dependent on that service.

   iv. Actions required for the start-up, restart or shutdown of a specific system or application.

   v. Actions performed for system or application backup.

   vi. Actions performed for system/ application recovery or restoration; and

d. All system and application administrators shall ensure that SOPs are updated at specified intervals or at the time of any system change(s).

e. The SOP shall facilitate building or rebuilding of the system and/ or application. There shall be enough detail in the SOP to eliminate non-compliance(s) with the operational (platform) standard when the build of system/ application is completed. Build and configuration checklists shall be used for this purpose.

f. Changes to operating procedures shall be carried out as per the Change Management Process.

6.3.2 Change Management

a. *Change Management Process* is applicable to any change that could impact confidentiality, integrity or availability of information processed by or stored in the information systems.

b. Changes in the systems/ environment shall be monitored for compliance with the established *Change Management Process*.

c. Change controls shall be applied to all security aspects of production applications and infrastructure.

d. Change(s) in the production systems/ environment shall be managed effectively to ensure that the security of the systems/ environments is not degraded.

e. The *Change Management Process* shall include the following: -

    i. Assessment of the potential impact, including security impact of the change(s) on critical systems.

    ii. Identification of the change authorisers.

    iii. Formal approval procedure for the proposed change(s).

    iv. Procedure for testing including security-testing of the change(s).

    v. Communication of details of change to all affected parties.

    vi. Recording of all the changes; and

    vii. Rollback procedure for aborting and recovering from failed change(s).

f. All third-party service providers are required to manage the change(s) to systems and services supplied to Bharti Real Estate as per the Change Management Process.

g. All approved changes on the critical systems shall be tested prior to implementing them on the production systems.

h. Change management Process of SO Partner shall be followed as they have been outsourced the device / service management.

6.3.3 Patch Management

Patches to the production systems shall be applied in a timely manner to ensure that the systems are running at their optimum level and threats from the spread of viruses, worms and malicious activities are reduced to an acceptable level. A formal *Patch Management Procedure* shall be established for applying patches to the information systems. All the critical patches that could affect the configuration of the critical information systems shall be subject to the *Change Management Process*.

The *Patch Management Procedure* shall ensure the following: -

a. Technical vulnerabilities for the information systems are dealt with in a timely manner.

b. Once a notification of a potential vulnerability is received, there is a process to identify the risk and the actions to be taken.

c. Roles and responsibilities are established and associated with technical patch/ vulnerability management.

d. Patches on sensitive and critical information system are tested before their application to production environment.

e. The systems at high risk are addressed on priority.

f. Timelines are defined to react to vulnerability notifications based on the risk and relevant technical notifications; and

g. The newly released security patches are applied within the stipulated timeframe.

h. We shall follow the process and procedure of SO Partner as Data Center management being outsourced to them.

6.3.4 Segregation of Duties

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. The HODs of all functions are required to ensure that no employee in their function is responsible for multiple duties such that it could lead to the circumventing of existing security controls. (For example, in IT and Networks, no employee shall be simultaneously responsible for more than one of the following duties- network management, system administration, systems development, change management, security administration, security audit.)

Where segregation of duties is not possible, approval of the HOD of the function should be obtained prior to allocating responsibilities to the employee. Further, compensating controls such as monitoring of activities, maintenance and review of audit logs (if required) and management supervision shall be put in place.

6.3.5 Separation of Development, Test and Operational Facilities

a. The production environment shall be logically separated from the development and test environments.

b. The Change Management Process shall be followed for implementing any change to the production environment.

c. Access to production, development and test environments shall be provided on the basis of segregation of duties.

d. Production data shall be sanitised and masked prior to its use in the test or development environments.

6.4. Third Party Service Delivery Management

6.4.1 Service Delivery

a. Third parties shall ensure that information security is implicitly integrated in all service delivery processes such as service level management, capacity management, IT service continuity management, availability management, financial management and supplier relationship management.

b. Third parties shall ensure that information security is implicitly integrated in all Service Support Processes such as service/help desk, incident management, problem management, configuration management, change management and release management.

c. IT and Networks functions shall ensure that service definitions, service delivery levels and security controls included in the third-party service delivery agreement and BRISP are adequately implemented, operated and maintained by the third parties.

d. IT and Networks functions shall conduct the reviews of third-party service delivery at specified intervals to ensure that third parties are meeting the agreed services levels.

6.4.2 Monitoring and Review of Third-Party Services

The IT functions shall establish a process to ensure the following: -

a. Services, reports and evidence provided by the third parties are monitored and reviewed at regular intervals.

b. Audits Reviews are conducted at specified intervals to assess the compliance of third-party services with the agreed contract and the BRISP are conducted at regular intervals, preferably once a quarter; and

c. Responsibilities for managing the relationship with third parties are assigned to a designated individual or team.

6.4.3 Managing Changes to Third Party Services

A documented procedure to control the changes to third party services shall be developed for managing such services considering the criticality of the involved information systems and business processes.

6.5. System Planning and Acceptance

6.5.1 Capacity Management

a. Projections of future capacity requirements for the existing and/ or new systems shall be planned by the IT functions in consultation with the following: -

   i. Asset owners of the existing systems; and

   ii. Heads of departments requiring the new system.

b. System/ application/ network administrators are required to monitor the capacity utilisation and project the future capacity requirements to ensure that adequate processing power and storage are available in accordance with the Capacity Management Process.

6.5.2 System Acceptance

a. Acceptance criteria for new information systems, upgrades and new versions shall be established.

b. Suitable tests of the systems shall be carried out during development and prior to acceptance.

c. Security clearance shall be obtained from the IT Head before any new information systems, upgrades and/or new versions are accepted.

6.6. Protection against Malicious Code

6.6.1 Controls Against Malicious Code

a. Procedures for controlling and managing malicious code shall be formalised and documented.

b. Procedures shall include prevention, detection, and recovery controls for malicious codes.

c. Detection, prevention, and recovery controls shall be implemented in all information systems to protect against malicious code.

d. Controls implemented on the information systems shall be capable of addressing the latest vulnerabilities and insecurities that could bring the system down or result in information disclosure or destruction.

6.7. Backup

For the continuity of business operations in the event of failures and/ or disaster, it is essential to have secondary copies of the data available. The IT functions are required to ensure that appropriate backup procedures are developed and implemented for specified IT systems and Network devices. The list of specified devices shall be prepared by IT functions.

6.7.1 Information Backup

a. Information backup and restoration procedures shall be established and implemented to ensure the availability of business information. The following shall be included in the *Backup and Restoration Procedure*: -

   i. Extent (e.g., incremental, differential, full back up) and frequency (backup schedule) of the backup.

   ii. Restoration testing procedure for critical information systems.

   iii. Duration for which the backup is to be maintained.

   iv. Responsibility of backup, restoration testing and media storage.

b. Restoration testing shall be conducted for the backed-up data at specified intervals to check the integrity and adequacy of the backup.

c. Backup operators shall store backup logs with appropriate access rights assigned to them. The backup operator shall carry out a log analysis for all failed backup and restorations.

d. Employees are responsible for backing up the data held in their workstations and laptops.

e. Business-critical data shall be duplicated. One copy shall remain onsite another should be replicated on the DR site. Backup appliances/Media will be used for backup.

f. Backup media/Appliances shall be used to take secondary backup and for subsequent backup testing (other than the replication on DR site as backup)

g. All backup media shall have uniquely identifiable labels attached to them.

6.8. Network Security Management

6.8.1 Network Controls

Controls shall be implemented by IT functions to protect the Bharti Real Estate network. The network controls shall ensure that the network documentation is maintained. Suitable information security controls shall be implemented in the infrastructure and systems.

The network controls shall include, but not limited to, the following: -

a. Logical segregation of networks as per the zoning architecture for secure zones, internal network zones, external network zones and Internet zones and also ensuring the access and connection restrictions.

b. Protection of critical networks/ information systems/ applications through a firewall against both external and internal users. The firewall shall be configured and managed to limit access only to authorised users.

c. Documentations related to the updated network diagrams, IP addressing, configuration of network devices and location of network devices.

d. Management of networks and associated equipment from a separate virtual local area network; and

e. Protection of the IT and Networks infrastructure against unauthorised access, modification and/ or destruction.

6.8.2 Wireless Local Area Network (WLAN)

The wireless infrastructure system shall be managed appropriately in order to provide protection to its information and information systems. The following controls shall be implemented to ensure WLAN security in accordance with the WLAN Standard and the WLAN Security Procedure given below: -

a. Separation of WLAN from the wired LAN by implementing a firewall.

b. Secure configuration of wireless communication devices including wireless access points and wireless client devices such as laptops/ workstations.

c. Implementation of a authentication mechanism for the clients connecting to the WLAN;

d. Implementation of appropriate physical and environmental security controls to protect wireless access points against theft and damage.

e. Implementation of appropriate security controls and detection mechanism to identify and respond to rogue access points, intruders and attacks directed over the WLAN; and

f. Maintenance and review of wireless network logs base on the incident criticality.

6.8.3 Firewall

Firewalls shall be deployed to limit the ingress and egress traffic in Bharti Real Estate network. Firewall Management includes all firewalls owned, rented, leased, or otherwise controlled by Bharti Real Estate. The Firewall Management Procedure given below: -

a. Firewall segmentation based on risk levels. Systems with similar risk level shall be put into one segment. (For example, De-Militarised Zone where publicly accessible systems are hosted, an internal local area network zone, a secure zone where critical servers/ databases/ network devices are located, etc.);

b. An updated & reviewed network diagram with all connections to and from the firewalls.

c. A documented list of services and ports required to be enabled for the business.

d. A documented procedure for firewall rule base creation, modification, performance monitoring, firewall backup and firewall change control.

e. Approval process for the creation of new rule base and/or modification in the existing rule base;

f. Enabling the audit logging on the firewall to ensure that all critical accesses and changes to firewall configuration and policy are tracked. These logs shall be regularly monitored ;

g. Deployment of approved intrusion prevention systems, as appropriate, along with the firewalls to detect/ prevent the intrusion and other unauthorised/ malicious activities; and

h. The intrusion prevention system log reports, which shall be produced in a defined format, shall be reviewed by Security SPOC of IT function at specified intervals.

6.8.4 Security of Network Services

a. The IT functions are required to identify the security features, service levels and management requirements of all network services included in any network services agreement, whether these services are provided in-house or outsourced.

b. The IT functions are required to prepare a checklist of the non-essential, default and vulnerable services for all information systems. Non-essential services shall be disabled on all information systems and the default and vulnerable services required for business operations shall be fixed by implementing alternative mitigation controls.

c. Changes to the security of network services shall follow a formal Change Management Process with an approval from the Security SPOC of IT functions prior to the implementation of change in the production environment.

6.9. Exchange of Information

6.9.1 Information Exchange Policies and Procedures

a. Appropriate security controls shall be implemented to exchange the business information or software assets with the third parties. The security controls shall include technical controls and contract/ agreements signed with the third parties.

b. Information asset owners shall be responsible for ensuring the implementation of the specified security controls on the information owned by them.

c. Employees and third-party staff shall exchange the information classified as ‘Strictly Confidential’, ‘Confidential’ and/ or ‘Internal’ with authorised personnel only.

d. Considering the Business requirement and to enable our Employees to interact / share and collaborate among themselves / with partners, all ports of laptop including but not limited to will be kept unrestricted i.e. USB/External Storage, HDMI / VGA / LAN Port / SD Card. The above-mentioned changes has been done post all due discussion & evaluation with the management.

e. Introduced the Data leak Prevention system which shall support the IT Team in order to Log / Monitor the activities.

6.9.2 Exchange Agreements

Agreement for the exchange of information/ software between Bharti Real Estate and third parties and customers shall be established.

6.10. Monitoring

6.10.1 Audit Logging

a. IT Function are required to ensure that the recording the critical user-activities, exceptions and security events are enabled and stored for reasonable periods to assist in future investigations and access control monitoring.

b. Logs/alerts shall be monitored and analysed for any possible unauthorised use of information systems.

c. Security controls shall be built to ensure the integrity of logs.

d. Access to audit trails and logs shall be provided to authorised users only and shall be password protected.

6.10.2 Monitoring System Use

a. The utilisation of information systems shall be monitored to ensure their continued and reliable operation.

b. A monitoring tool shall be implemented for log storage and monitoring. The log monitoring tool shall store and monitor the following: -

i. Authorised access.

ii. All privileged operations.

iii. Unauthorised access attempts; and

c. The results of the monitoring activities shall be reviewed at specified intervals. The intervals shall be decided as per the criticality of the information systems.

6.10.3 Protection of Log Information

a. Log information shall be protected against unauthorised access, alterations, and operational problems. Access to logs shall be provided on ‘need-to-know’ and ‘need-to-have’ basis.

b. Appropriate controls shall be implemented to prevent: -

i. Alterations of the message types that are recorded.

ii. Alterations or deletions of the log files; and

iii. Exceeding the storage capacity of the logging media.

6.10.4 Administrator and Operator Logs

a. Information systems shall be configured in such a way that the system administrator and system operator activities are logged.

b. These users shall not have access rights to access administrator and operator logs.

6.10.5 Fault Logging

a. The IT Helpdesk is required to maintain logs of all the faults reported by the users related to the data processing problems and communication systems.

b. The IT Helpdesk shall be responsible to ensure such issues are reported to the Incident Response Team.

c. The Incident Response Team shall ensure that the necessary corrective actions are taken, and the root-cause analysis is carried out in case of major faults as per *Information Security Incident Management Process* and a report is presented to the Security SPOC from IT/ Networks functions.

6.10.6 Clock Synchronisation

a. All computer clocks shall be set to an agreed standard. As some clocks are known to drift with time, there shall be a procedure that checks for and corrects any significant variation.

b. The clocks of the critical servers and network devices shall be synchronised with a Network Time Protocol (NTP) server.

c. The correct interpretation of the date/ time format shall be ensured. The format shall be identical across all servers and network devices.

7. Access Control Policy

7.1. Introduction

The *Access Control Policy* defines the controls that need to be implemented and maintained to protect information assets against unauthorised access that poses 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 Bharti Real Estate.

7.1.1 Responsibility

It is the responsibility of the IT functions to implement and maintain the controls defined in the *Access Control Policy*.

It is the responsibility of the HR function to coordinate with the IT/ Networks function for User ID management controls.

7.2. Policy Statement and Objective

Access to information assets shall be controlled, based on the business and security requirements and commensurate with the asset classification. Access controls shall be deployed on the principle of 'deny all unless explicitly permitted' to protect the information from unauthorised access.

The objectives of the *Access Control Policy* are to: -

a. Restrict access to the information assets as per the business requirement.

b. Prevent unauthorised access to information systems, network services, operating systems and information held in database and application systems.

c. Ensure that the security controls are in place while using mobile computing and tele-working facilities; and

d. Ensure that information access controls are implemented to meet any relevant contractual requirements, as applicable.

7.3. User Access Management

The allocation of access rights to information systems and services shall be done in accordance with the *User Access Management Procedure*. The procedure encompasses all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Special attention has been given, where required, to control the allocation of privileged access rights, which could allow users to override the system controls.

7.3.1 User Identity Management

The 'User' registration and de-registration of employees and third-party staff shall be done in accordance with the *User Access Management Procedure* for granting access to all multi-user information systems including Operating Systems, Applications, Databases, Network Devices. The following shall be implemented: -

a. A unique user ID for all users having access to the information systems.

b. Approval from the of the function that is dealing with the third party prior to the creation user IDs of third party staff;

c. Obtaining appropriate authorisation prior to creating user IDs.

d. Assigning of access privileges to the user only in accordance with the user's role and appropriate approval.

e. Keeping audit trails for all requests for addition, modification or deletion of user accounts/ IDs and access rights.

f. Reviewing user accounts at specified intervals to identify and facilitate removal/ deactivation of inactive accounts or accounts that have not been used for a longer duration; and

g. Reviewing results of user account reviews at specified intervals, including subsequent actions to provide an audit trail.

7.3.2 Privilege Management

Creation and allocation of privileged user accounts/ IDs on the information systems shall be controlled through a formal authorisation process in accordance with the *User Access Management Procedure*. The procedure shall ensure the following: -

a. The privilege associated with each system (e.g. Operating Systems, Databases, Applications) and their corresponding users are identified.

b. Privileges are allocated to individuals on a 'need-to-have' basis in strict adherence to the authorisation process for privilege access.

c. A record of all privilege accounts used on the information systems is maintained.

d. Changes made to privileged accounts are logged; and

e. The logs are reviewed at a specified periodicity.

f. Privilege User account shall be removed if Time completed, Pre-Closure Request, Violation, Change in Roles/Responsibility etc.

7.3.3 Password Management Policy

Passwords are strings of characters that are input to a system to authenticate an identity and/or authority and/or access rights.

Appropriate technical specifications for password management, as specified in *Password Management Standard*, shall be implemented on the information systems and applications.

7.3.4 Review of User Access Rights

The review of user access rights shall consider the following: -

a. User access rights are reviewed at regular intervals for users having access to critical systems/ applications.

b. Whenever a user is transferred from one function/ geography to another function/ geography within Bharti Real Estate, the user access rights are to be revoked and re-allocated appropriately.

c. Authorisations for special privileged access rights are reviewed at regular intervals.

d. Privilege allocations are to be checked at regular intervals to ensure that unauthorised privileges have not been obtained; and

e. Changes to privileged accounts are to be logged for periodic reviews.

7.4. User Responsibilities for Access Management

All employees and third-party staff with access to information assets are required to understand their responsibilities for maintaining the effective access controls, particularly regarding the use of passwords and the security of user equipment.

7.4.1 Clear Desk and Clear Screen

The IT functions are required to implement the appropriate technological controls to lock the screen of the information systems when these are unattended beyond a specified duration. It is the responsibility of all employees and third-party staff to adhere to the clear desk and clear screen standards specified in the Information Security policy.

7.4.2 Password Use

Employees and third-party staff are required to: -

a. Keep their passwords confidential and refrain from sharing them with others.

b. Change their passwords whenever there is any indication of a possible compromise of the system or password; and

c. Change passwords at regular intervals or based on the number of accesses (passwords for privileged accounts shall be changed more frequently than normal passwords).

7.4.3 Unattended User Equipment

All employees and third-party staff with access to information assets shall be made aware of the information security requirements and procedures for protecting unattended equipment, as well as their responsibilities for implementing such protection. The users are required to do the following: -

a. Terminate active sessions when finished or implement an appropriate equipment locking mechanism; and

b. Logout from the workstation, servers and/ or network device when the session is finished.

7.5. Network Access Control

Appropriate controls for user access to networks and network services shall be applied. The controls shall ensure that: -

a. Appropriate interfaces are created to segregate the Bharti Real Estate’s networks from the networks owned by other organisations and public networks.

b. Appropriate authentication mechanisms are applied for users and information systems.

c. Control of the user access to information services is enforced.

d. Users are provided access only to the services that they are specifically authorised to use.

e. Authorisation process is developed and implemented to ensure that only users who are allowed can access the network segments and services.

f. Business applications are accessible on the network only through the approved network services and segments; and

7.5.1 Remote Access to IT Networks Control Policy

Adequate security controls shall be implemented to authenticate the user for remote access. There shall be a formal procedure to manage the remote access connections. In accordance with *the Remote Access Control Procedure*, it shall be ensured that: -

a. Remote access connections to the Bharti Real Estate IT network are provided to authorised users only and appropriate controls implemented to maintain the confidentiality, integrity, and availability of information.

b. Remote access to the network of Bharti Real Estate is allowed through secure channels (VPN) only.

c. User with authentic credential shall only be able to access ERP and other network directory.

7.5.2 Segregation in Networks

The security of the Bharti Real Estate network shall be divided into separate logical network domains, e.g. internal network domains, external network domains, etc. Each of these domains shall be protected by a defined security perimeter. A graduated set of controls shall be applied in different logical network domains to further segregate network security environments, e.g. De-militarised Zone where publicly accessible systems are hosted, an internal local area network zone, a secure zone where critical servers/ databases/ network devices are located, etc.

Network Zones and Data Flow Access Controls shall be designed with the following considerations: -

a. Network Zone Definitions.

b. Network Zone Security Hierarchy.

c. User Profiles.

d. Host Systems Profiles.

e. Zone to Zone Data Traffic Flow Control.

f. User to Network Zones Data Traffic Flow Control; and

g. Host Systems to Network Zones Data Traffic Flow Control.

7.5.3 Network Connection Control

a. For shared networks, especially those extending across the boundaries of Bharti Real Estate, the capability of the users to connect to the network shall be restricted as per the Access Controls Policy and/ or the requirements of business application(s).

b. The download from the Internet through insecure file transfer application(s) is not allowed. If there is a business requirement for such downloads, the secure file transfer protocol shall be used for such activities with prior authorisation from the Security SPOC of the IT/ Networks functions.

c. Insecure file transfer uploads to the Internet shall not be allowed. The only exclusion to this is when data like configuration details, fault logs, screen shots, (but not limited to these), is required to be uploaded to a manufacturer, service provider or other such authorised support third parties for the purpose of diagnostics and fault repairs. Such uploads may be executed only if authorised by the owner of the equipment and the Security SPOCs of the IT and/ or Networks functions.

d. Use of personal mail services shall be discretionary in Bharti Real Estate.

7.5.4 Network Routing Control

a. Appropriate routing controls meeting the requirements of the Access Controls Policy shall be implemented.

b. Controls that filter the traffic by means of pre-defined tables or rules shall be implemented through network gateways.

c. Routing controls shall be defined based on the source and destination address checking mechanism.

d. Firewalls shall mask the internal IP addresses for outbound Internet access.

7.5.5 Operating System Control

Adequate security controls shall be implemented on the information systems to restrict access to operating systems to authorised users only. The controls shall authenticate the authorised users as per the Access Control Policy.

7.5.6 Secure Log-on Procedure

The operating systems of servers, workstations and/ or network devices shall be controlled through a log-on procedure. The log-on procedure shall not disclose any information of the system. The remote log-on procedure shall be designed with consideration of encryption of information during its transmission. A secure network channel shall be established for the remote access.

7.5.7 User Identification and Authentication

a. Employees and third-party staff who have access to the information assets shall be assigned a unique login ID.

b. An authentication system shall be implemented to identify the user. As an exception, group ID may be used but approval from the Security SPOC of IT function shall be obtained and documented for the same.

c. For the information systems that contain critical business information, authentication and identity verification are required.

7.5.8 Password Management System

IT and Networks functions shall implement a password management system for the users. The password management system shall be based on the Authentication, Authorisation and Accountability (AAA) principle and capable of enforcing the *Password Management Standard*.

7.5.9 Use of System Utilities

Any use of utility programs that could override the system and application controls shall be restricted and tightly controlled. Only utilities authorised for the remote management of the servers, workstations and network devices shall be used. IT functions shall ensure that vendor default utilities are disabled during new server, network device or workstation commissioning. If for troubleshooting purpose there is a need to use these utilities, administrators of the servers and network devices shall ensure that such utilities are enabled for an authorised activity and are disabled immediately after the use. They shall ensure that activities carried out by using such utilities are logged.

7.5.10 Session Time-Out

Information systems and applications that are accessed from the external networks and Internet shall be equipped with session time-out control to clear the session screen and terminate both the application and the network sessions after 15 minutes of inactivity, unless defined otherwise.

7.6. Application and Information Access Control

Logical access to the application software shall be restricted to authorised users only. The appropriate security controls shall be used to restrict access to the application systems of Bharti Real Estate. All applications shall be tested for information security. An application security assessment shall be conducted for the critical applications at regular intervals. Clearance from the IT Head shall be obtained prior to deploying application in the production environment.

7.6.1 Information Access Restriction

IT function shall restrict access to information and application systems as per the *Access Control Policy*. System administrator or the person performing the equivalent role is required to maintain the updated user access matrix with privileges assigned to the users. Asset owner or security SPOC of IT function shall review the access rights at regular intervals.

7.6.2 Sensitive System Isolation

Applications that are used for processing and/ or storing the critical information shall not be hosted on the shared server. All such applications shall be identified and documented by the application administrator.

7.6.3 Content Management

The IT functions shall implement content filtering measures to filter websites for legal and regulatory compliance. Such websites shall include, but are not limited to, sites with racial content, pornographic sites, etc. Suitable content filtering tools shall be used for this purpose.

Suitable technical controls shall be implemented to maintain the integrity of the contents that are stored in the critical information systems such as Database, application systems, etc.

In information systems where third parties are uploading the contents for providing value added services, it shall be ensured that strong content-checking mechanism are employed to ensure that such contents do not have hidden viruses, worms, malicious codes, backdoors and/or executables that could harm the information systems or the customer's device that downloads these contents.

7.7. Mobile Computing and Teleworking

7.7.1 Mobile Computing and Communication

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

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

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

d. Third party staff shall not connect their computing devices to the wired or wireless network of Bharti Real Estate, unless authorised by the Security SPOC of IT function.

8. Information Systems Acquisition, Development & Maintenance Policy

8.1. Introduction

The *Information Systems Acquisition, Development and Maintenance Policy* defines the security requirements that need to be identified and integrated during the development and maintenance of applications, software, products and/or services.

8.1.1 Responsibility

The development, testing, operations, and maintenance teams of IT functions are responsible for the implementation and maintenance of the controls defined in this policy.

The IT functions are also responsible for ensuring the enforcement for the implementation of this policy during the acquisition, development and maintenance of application software, system software, products and/or services.

8.2. Policy Statement and Objective

Appropriate security controls shall be integrated during acquisition, development, deployment and maintenance of the application software, system software, products and/or services ensuring confidentiality, integrity and availability of the information.

The objectives of this policy are to: -

a. Strengthen confidentiality, integrity and availability of information.

b. Ensure that information security is an integral part of the application software, system software, products and/or services.

c. Ensure integrity of system files; and

d. Maintain the information security of application system software and information during its lifecycle.

8.3. Information Security Requirements in New Initiatives

a. All functions are required to ensure that information security requirements are established for the following: -

i. Initiating any new projects.

ii. Developing/acquiring new systems or services.

iii. Carrying out/facilitating enhancements to systems/services; and

iv. Procuring new software products and services and deployment of new information technology initiatives.

b. Security control specifications shall be analysed during the design and development stage or enhancement to application systems and in the pre-purchasing stage, when a product/service is being evaluated so that security is incorporated into the products/services while they are being designed or procured.

c. Every new application, whether it is developed in-house or is a Commercial Off the Shelf Product, shall be assessed from all the following perspectives: -

i. Business Process Controls

ii. Access Controls

iii. Authorisation Controls

iv. Authentication Controls

v. Application Controls

vi. Database Controls

vii. System Controls

viii. Network Controls

d. All new applications shall be formally reviewed for compliance with the BRISP and a sign off on the same shall be obtained from the IT Head before deploying in production environment.

8.3.1 Input Data Validation

a. Controls shall be built in the application systems to validate the data entered into it.

b. System requirements specification shall include these controls in the application under consideration.

8.3.2 Control of Internal Processing

a. System requirements specification shall include controls of internal processing, such as data integrity checks on the data downloaded/ uploaded and audit trails in the application under consideration, to prevent corruption of data.

b. The applications shall include controls such as out-of-range checking, checking for invalid characters in data fields, missing or incomplete data, exceeding upper and lower data volume limits and inconsistent data control.

8.3.3 Message Integrity

Message integrity protection requirements in the applications and information systems shall be identified and controls for integrity shall be implemented.

8.3.4 Output Data Validation

During the construction stage of the application systems, the data generated from the application system after processing the stored information shall be validated to ensure that output is correct and appropriate.

8.4. Security of System Files

8.4.1 Control of Operational Software

a. Appropriate controls shall be implemented to deploy the software on operational/production systems to minimise the risk of corruption of these systems.

b. Access to installed software on operational/production systems shall be restricted to the authorised personnel only.

c. Modifications to the operational environment shall be logged and previous versions be maintained for contingency/ roll back purpose.

d. Operational/Production systems shall hold only executable code.

e. New executable code shall be implemented in the operational/production environment only after successful completion of testing and user acceptance of the system in a separate controlled environment.

f. All upgrades and applications of service packs shall be carried out after appropriate testing and evaluating the additional security measures provided by the vendor.

8.4.2 Protection of System Test Data

a. Acceptance tests shall be carried out using the test data, which shall be similar to the operational data.

b. The software development team shall ensure that test data is secured and sanitised during testing.

c. Separate authorisations shall be required every time the operational data is used for testing purposes.

8.4.3 Access Control to Program Source Code

a. Access to the program source of operational systems shall be controlled to prevent any corruption of the application programs.

b. IT and Networks functions shall use configuration management process and identify program librarians to maintain the source libraries of the operational application systems in configuration management database.

c. All updates or issue of the program sources to developers shall be carried out through an authorised request.

d. Configuration management database shall maintain the version control of all programs and change control procedures need to be followed for any modifications to the program source library.

8.5. Security in Development and Support Processes

Changes to application systems shall be carried out in a controlled manner as per the *Change Management Process*. The *Change Management Process* shall include, but not be limited to, the following: -

a. Recording changes in change request forms and approval of change requests.

b. Impact assessment due to the change.

c. Executing and testing changes.

d. User acceptance testing, where applicable.

e. Rollback procedures; and

f. Documentation of changes.

Changes shall not be carried out in production environment directly; all changes shall be applied to development/ test environment.

8.5.1 Technical Review of Applications after Operating System Changes

a. All operating systems shall be periodically updated with the new release or patches from the vendor.

b. New releases/ Patches pertaining to the operating system shall be tested before being implemented in the production environment to ensure that there is no adverse impact on operation, application controls or security.

8.5.2 Restrictions on Changes to Software Packages

a. Vendor-supplied software packages shall not be modified as far as possible without consulting the vendor.

b. Any requirement for change to such software shall undergo the Change Management Process. If changes are essential, then original software shall be retained, and changes could be applied to a clearly identified copy.

8.5.3 Information Leakage

a. In order to avoid risk of the introduction of covert channels and/ or Trojan code, the application and software shall be appropriately evaluated before implementation.

b. Appropriate controls shall be introduced to avoid unauthorised access and modification to program source code after installation. In-house developed software shall undergo testing before being put to operational use.

8.5.4 Outsourced Software Development

a. For the customised (not off-the-shelf/ standard offerings) software developed by third parties, arrangements pertaining to licensing, code ownership and intellectual property rights shall be documented in the contract between Bharti Real Estate and the third party.

b. The contract shall include that Bharti Real Estate reserves the right to audit quality and accuracy of software development and testing.

8.6. Technical Vulnerability Management

8.6.1 Control of Technical Vulnerabilities

a. The IT functions shall identify and document all technical vulnerabilities of information systems and evaluate the exposure to such vulnerabilities. Appropriate measures shall be taken to mitigate the associated risk.

b. The IT functions shall define and establish the roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability assessment and vulnerability closure.

c. IT Team shall follow a Vulnerability Assessment cycle from October to October considering the normal operations.

8.6.2 Cyber Security Operation Process Overview:

a. The Cyber Security Operation Process collaborates with the SOC (Security Operation Center) for enhanced security measures. As Bharti Airtel have expertise in this and large to provide support as services hence, we have outsourced the SOC services to bharti Airtel for 24x7 support and monitoring of security services. Policy is aligned with the supplier SOC standard norms.

b. SOC involvement ensures a comprehensive approach to security management.

Role of Cyber Threat Intelligence:

c. **Threat Intelligence plays a vital role in safeguarding the client organization.**

d. **Provides timely alerts about the latest observed threats worldwide with help of SIEM tool.**

e. **Enhances the organization's ability to respond effectively to emerging security risks.**

Utilization of Seceon (SIEM Solution):

f. **Seceon functions as a Security Information Event Management (SIEM) solution**

g. **Collects logs from various sources within the Bharti Real Estate environment.**

h. **Performs proactive tasks such as event and flow collection, normalization, correlation, and secure storage.**

Key Functions of Seceon:

i. **Event and flow collection**

j. **Normalization of collected data.**

k. **Correlation of security events**

l. **Secure storage of logs**

Cyber Security Alert Generation Process:

m. **Logs are validated by Seceon.**

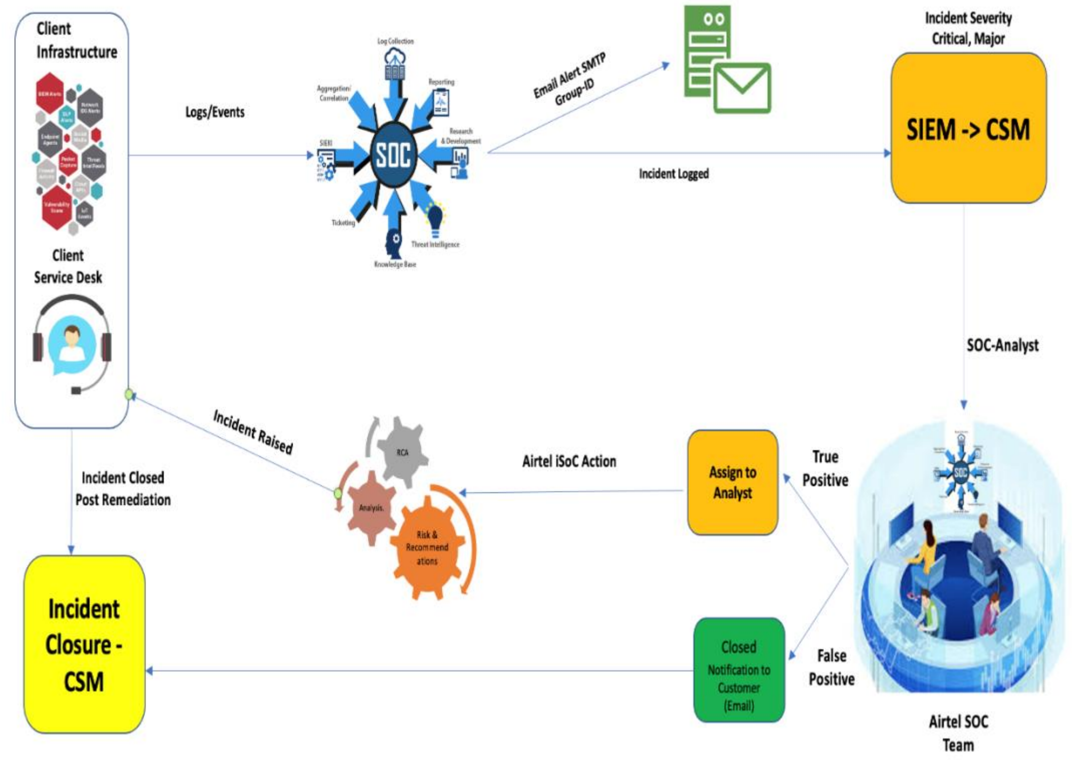
n. **Alerts are generated proactively based on logs collected.**

o. **Bharti Real Estate Team is promptly informed of the generated alerts.**

The diagram serves as a valuable resource for Cyber Security Airtel SOC Analysts and the Bharti Real Estate Team, offering a clear and concise overview of investigations related to targeted attacks. It outlines distinct responsibilities assigned to individuals involved in mitigating such issues. This visual aid enhances collaboration and understanding among team members, facilitating a streamlined and effective response to potential security threats.

Note: **As we have outsourced SOC managed services to Airtel so on basis of given below diagram, Policy is aligned with the supplier SOC standard norms.**

Airtel SOC | Incident Management Lifecycle



9. Information Security Incident Management Policy

9.1. Introduction

The *Information Security Incident Management Policy* provides directions to develop and implement the Information Security Incident Management Process for networks and computers, improving user security awareness, early detection and mitigation of security incidents and suggesting the actions that can be taken to reduce the risk due to security incidents.

9.1.1 Responsibility

It is the responsibility of ISSC to establish a Central Incident Response Team (IRT includes Functional Domain, local helpdesk, Application helpdesk) having representation from all the domains.

It is the responsibility of the IT Head at HO to appoint representatives from each domain to act as the Incident Response Team.

It is the responsibility of all employees and third-party staff also to report any security incident that they observe or suspect to the IT Helpdesk. They shall also send an email to my.it@bhartirealty.com this regard.

9.2. Policy Statement and Objective

All security breaches or attempts to breach and all discovered security weaknesses in information systems and processing facilities shall be reported. The Information Security Incident Management Process shall ensure that all reported security breaches or weaknesses are responded to promptly and actions taken to prevent reoccurrence.

The objectives of this policy are to: -

a. Develop the proactive measures to minimise the impact of any Incident on information systems and processing facilities.

b. Create the awareness and encourage the users to report the security weaknesses and/ or incident that they identify.

c. Enable the proactive management of problems by capturing data that can be used to analyse trends and problems areas, thereby preventing the security incidents to occur; and

d. Learning from the incidents and continually improving the information security posture within Bharti Real Estate.

9.3. Incident Identification

a. A security incident could be defined as the act of violating the security policy. The following is an illustrative list of what actions can be classified as incidents: -

   i. Attempts to gain unauthorised access to a system or its data; masquerading, spoofing as authorised users;

   ii. Unwanted disruption or denial of service;

   iii. Unauthorised use of a system for the processing, transmitting or storing data by authorised/ unauthorised users;

   iv. Changes to system hardware, firmware or software characteristics and data without the knowledge of application owner; and/ or

   v. Existence of unknown user accounts.

b. Appropriate detective mechanism shall be designed for timely detection of information security incidents.

c. Preventive controls shall be put in place to minimise the occurrence of information security incidents.

d. All information security incidents shall be recorded as per the Information Security Incident Management Process.

e. Appropriate forensic methods shall be applied, whenever required, to collect evidence in the course of investigation of information security incidents. This shall be done by a trained forensics investigator if needed.

9.4. Reporting Information Security Events and Weakness

a. A formal Information Security Incident Management Process including incident reporting, incident response, escalation and incident resolution shall be established.

b. Employees and third-party staff shall be made aware of their responsibilities and process for reporting the security incidents that they observe or suspect.

c. Responsibilities shall include and explicitly state that they shall not be involved in committing security breaches or attempting to prove the suspected security incidents.

d. In addition, the users shall not test the existence of vulnerability in any information system and/ or facility.

9.5. Learning from Information Security Incidents

a. The Incident Response Team shall establish a knowledge base for the information gained from the evaluation of all information security incidents.

b. The knowledge base shall be referred to for incident handling and as a learning source of information security incidents.

10. Business Continuity Management Policy

10.1. Introduction

Bharti Real Estate recognises the criticality and need of its business and understands the importance of the availability of its information systems and telecom services. The *Business Continuity Management Policy* defines the controls to establish a framework to counteract interruptions to business activities and to protect the critical business processes from the effects of business disruptions such as major failures, disasters, etc. and their timely resumption. The details on the various aspects of business continuity management are documented in the Business Continuity Plan Document.

10.1.1 Responsibility

It is the responsibility of the ISSC to establish the Business Continuity Task Force at the Bharti Real Estate office.

It is the responsibility of the ISSC at HO to function as the Business Continuity Task Force.

The Business Continuity Task Forces at the Bharti Real Estate HO shall be responsible for the development and implementation of the controls defined in this policy in their respective jurisdiction.

10.2. Policy Statement and Objective

Application systems and business processes that are critical to the business shall be planned for continuity of operations in the event of business disruptions. The cost effectiveness and fitness for purpose of countermeasures to be implemented shall be considered and continually reviewed as part of normal management responsibility.

The objective of business continuity is to promote organisational survival by ensuring that critical business processes can continue, or be recovered in a timely manner, following a disruption, thus ensuring:-

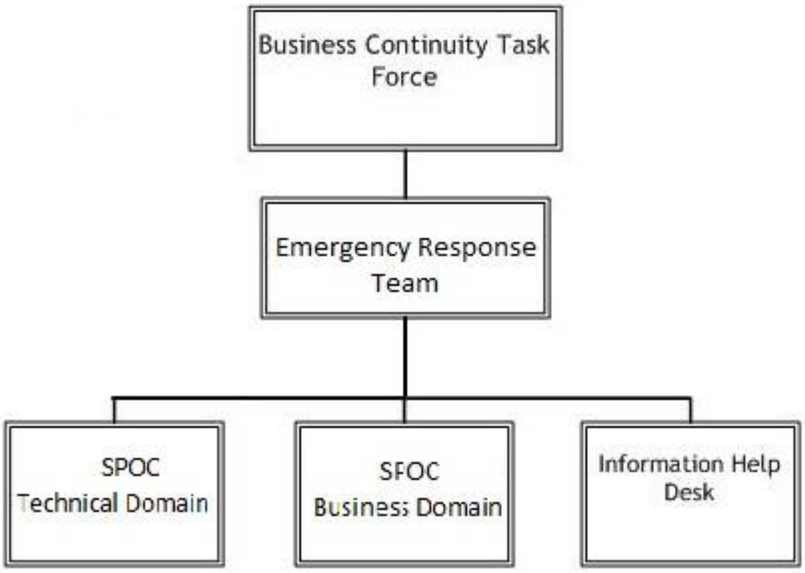
a. Operations are not adversely affected, thus maintaining the quality of management and meeting statutory and regulatory requirements of the business;

b. Customer expectations and quality of services continue to be met, or managed, in such a way that customers are retained and new business opportunities met; and

c. Reputation and image to stakeholders and the public are not negatively affected following business disruption.

10.3. Business Continuity Task Force (BCTF)

10.3.1 Business Continuity Task Force Structure



The Business Continuity Task Force shall comprise the following:-

Emergency Reponses Team.

a. SPOC from All Technical Domain

b. SPOC from all Business Domain.

c. Information Help Desk.

The structure and responsibilities of all teams of Business Continuity Task Force are defined in the later sections of the policy.

10.3.2 Business Continuity Task Force Responsibilities

The Business Continuity Task Force shall be primarily responsible for the following:-

a. Ensuring that a comprehensive Business Analysis is carried out for the critical business processes to prioritise the business functions by assessing the potential quantitative (financial) and qualitative (non-financial) impact that might result, if Bharti Real Estate was to experience a business continuity event;

b. Business Continuity Planning Framework include the following:-

   i. A consolidated and consistent approach for the continuity of all important business processes, applications and information processing facilities;

   ii. Controls that are required to ensure the availability and security of information and information systems; and

   iii. Fallback procedures and the condition for the activation of the framework as well as individual responsibility for executing each component of the Business Continuity Management Plan.

c. Developing Business Continuity Management plan that also includes controls required for the identification and mitigation of information security risks, in addition to the general risks, to limit the consequences of damaging incidents and to ensure that information required for the business processes is readily available; and

d. Ensuring the availability of information considering Recovery Time Objective (RTO), Recovery Point Objective (RPO) and information security requirements for critical applications.

10.3.3 Emergency Response Team (ERT)

This function involves gathering relevant information and options from the Operations and Support Team to enable accurate decision making and to delegate and follow up tasks to ensure on-ground implementation of actions.

A. Emergency Response Team Structure

Team shall comprise the following members:

a. SPOC from – IT Infrastructure team.

b. SPOC from – Application team.

c. SPOC from - Finance and Business Integration;

B. Emergency Response Team Responsibilities

The ERT shall be responsible for the following:-

a. Managing and co-ordinating the response to, and recovery from, a crisis;

b. Taking emergency actions;

c. Conducting situation assessment;

d. Activating the Business Continuity Plan;

e. Ensuring constant status monitoring; and

f. Enabling recovery finalisation.

10.3.4 Information Help Desk

The role of Information Help Desk is to notify and continuously update business continuity activities to Emergency Response Team and any other supporting parties in event of a disruption event.

A. Information Help Desk Structure

Existing IT Helpdesk shall function as the Information Help Desk for Business Continuity Management.

B. Information Help Desk Responsibilities

Information Help Desk shall be responsible for the following:-

a. Receiving information about the event on a continuous basis from ERT; and

b. Passing relevant information.

10.4. Information Security in Business Continuity Plan

a. Information security requirements shall be integrated in the Business Continuity Plan.

b. The Business Continuity Plan shall include information risk assessment, prioritisation and treatment for the critical applications and the supporting infrastructure.

c. The Business Continuity Management Plan shall have the ability to identify the impact of interruptions caused by information security incidents on business.

d. A thorough risk assessment shall be carried out for all assets required for business continuity, considering all the events that can cause disruption to the business processes. The considered events shall include, but are not limited to, man-made error, man-made disaster, natural disaster and technical failure, etc.

10.5. Testing, Maintaining and Re-assessing Business Continuity Plans

The Business Continuity Task Force shall ensure that:-

a. The Business Continuity Plan is tested at defined intervals;

b. The Business Continuity Plan is effective;

c. The results of the testing are recorded and maintained for improving on the developed Business Continuity Plan.

10.6. Disaster Declaration and Media Management Plan

Only the Emergency Response Team (ERT) shall be empowered to declare a Business Continuity event. This declaration shall be based on the following:-

a. The initial report of the Damage Assessment Team;

b. The expected time to recover normal operations;

c. The expected intensity of the disruption; and/or

d. Analysis of any other relevant facts.

10.6.1 Internal Communication

A preliminary internal announcement shall be made by the ERT to communicate the situation responsibly and accurately to the employees of Bharti Real Estate immediately following the declaration of such an event.

10.6.2 Public Communication

Only the authorised spokesperson from the Marketing and Communication function of Bharti Real Estate shall speak to the press on the occurrence of a business disruption event.

11. E-mail Security Policy

11.1 Introduction

The *E-mail Security Policy* provides the directions to ensure that the E-mail system is not vulnerable to interception, modification, interruption and/ or misuse. However, the E-mail communication would be made available to Security Agencies/Licensor on demand.

11.1.1 Responsibility

The IT function is required to implement appropriate controls ensuring prevention of interception, modification, interruption of the E-mail system.

All employees and third party staff using the E-mail system of Bharti Real Estate are required to adhere to the E-mail Security Policy.

11.2. Policy Statement and Objective

As a productivity enhancement tool, Bharti Real Estate encourages the business user to use electronic messaging systems. E-mail security is of prime importance hence Email Security tool (Preventing from SPAM, URL Sandboxing, content filter & AntiSpoofing, encryption etc) and user level controls shall be implemented to maintain the Security, confidentiality, integrity and availability of the E-mail system.

11.2.1 Authorised Use of E-mail

a. All messages generated by the E-mail System are considered to be the property of Bharti Real Estate. The E-mail system shall be used for business purposes only. However, the personal use of the E-mail systems is allowed to a reasonable extent as long as that does not damage the information and/ or reputation of Bharti Real Estate.

b. If users receive any offensive or unsolicited material from external sources, they shall not forward/ redistribute it to either other employees or third party staff.

c. All Employees are authorised to use the Email Services on their personal Mobile/iPADs.

11.2.2 Prohibited Use of E-mail

The use of the E-mail System is restricted for the following:-

a. Charitable fundraising campaigns, political advocacy efforts, private business activities or personal amusement and entertainment;

b. Creating or distributing any disruptive or offensive messages, including offensive comments about race, gender, hair colour, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs or national origin;

c. Forwarding or sending messages that have racial or sexual slur, political or religious solicitations or any other message that could damage the reputation of Bharti Real Estate;

d. Transmitting any material that potentially contains viruses, Trojan horses, worms, time bombs or any other harmful or malicious program;

e. Defaming abusing, harassing, stalking, threatening or otherwise violating any legal and privacy laws;

f. Using it in connection with surveys, contests, chain letters, junk E-mail, spamming, or any duplicative or unsolicited messages; or

g. Mail-bombing the other users.

11.3. User Accountability

a. Users shall not use any unauthorised web-mail services or portals.

b. Users shall not share their email passwords with others under any circumstances.

c. Users shall choose quality passwords which are compliant with the *Password Management Policy (Refer section 7.3.3)*.

11.3.1 User Identity

a. Misrepresenting, obscuring, suppressing or replacing another user's identity on an electronic communications system is forbidden;

b. The user name, electronic mail address, organisational affiliation and other information related to electronic messages or postings shall reflect the actual originator of the messages or postings; and

c. At a minimum, users shall provide their name and phone numbers in all electronic communications. Electronic mail 'signatures' indicating job title, company affiliation, address and the other particulars are recommended for all E-mail messages.

11.3.2 Electronic Mail Encryption

a. All users shall be aware that electronic communications through the E-mail systems are not encrypted by default, if they need to send any information marked as ‘Confidential’ or ‘Strictly Confidential’, it is recommended that they encrypt the e-mail before sending it.

11.3.3 Contents of Electronic Messages

a. Users shall not use profanity, obscenities or derogatory remarks in electronic mail. The users caught in such action shall be subject to consequence management.

b. All E-mail communications made by E-mail users shall be consistent with the Code of Conduct of Bharti Real Estate.

11.4. Disclosure of Content

a. It may be necessary for the technical support personnel to review the content of an individual user's communications during the course of problem resolution. Approval by the relevant Security SPOC shall be required for all such reviews.

b. Technical support personnel shall not review the content of an individual’s communications out of personal curiosity.

c. Regardless of the circumstances, the E-mail administrator or his team members shall not ask any user to reveal his/ her password. Users are advised not to reveal their password to anyone.

11.4.1 Attachments and Virus Protection

a. All malicious attachment shall be quarantined and deleted at the E-mail gateway/ server end. The E-mail administrator shall document malicious file extensions that need to be blocked at the E-mail gateway/ server level and ensure that these are blocked.

b. The E-mail administrator shall implement E-mail content filtering and virus protection software at the E-mail gateway/ server.

11.4.2 Public Representations

a. No E-mail message related to Bharti Real Estate shall be used for advertisement or public representation.

b. If users are concerned by an excessive amount of spam from a particular organisation or electronic mail address, they shall raise a security incident as per the *Information Security Incident Management Process*.

11.5. Archival Storage and User Backup

a. All official E-mail messages containing formal management approval, authorisation, delegation or handing over of responsibility or similar transactions shall be copied to the Archival Records.

b. If an electronic mail message contains information relevant to the completion of a business transaction or could be produced as evidence for a critical decision, it shall be appropriately retained for future reference.

c. The users shall regularly move their important E-mail messages to Archive files at the E-mail client end. The server end of the E-mail system is not intended for archival storage of the information.

11.6. Contracts Confirmation

a. All contracts formed through electronic messaging shall be formalised and confirmed via paper documents within the agreed time frame.

b. Users shall not employ scanned versions of hand-rendered signatures to give the impression that an electronic mail message or other electronic communications was signed by the sender.

11.7. Disclaimer

An approved disclaimer shall be appended to all electronic messages intended for domains other than Bharti Real Estate.

11.8. Monitoring and Enforcement

a. The users shall have no expectation of privacy in anything they store, send or receive on the E-mail system. Bharti Real Estate reserves the right to monitor all the messages without prior notice.

b. Users of the E-mail system are required to comply with the *E-mail Security Policy*.

11.9. Group E-mail ID Management Policy

As per the *E-mail Security Policy*, a unique e-mail ID shall be assigned to each user within Bharti Real Estate. However, depending upon the business need it may be required to have group E-mail ID. These group IDs shall be classified in two categories, ‘Restricted’ and ‘Public’ and it shall be ensured that controls are put in place to manage such group IDs.

Group E-mail ID management in Bharti Real Estate shall be done separately for both ‘Restricted’ and ‘Public’ group IDs. However, an approval from the Security SPOC of IT function shall be taken prior to creating any group ID.

The functional Security SPOC (Single Point of Contact) is responsible for validating the justification for group e-mail ID creation requests and providing approvals. The owner of Restricted group IDs is responsible for addition and deletion of members in the group ID. The HR&A/ Internal Communication function is responsible for verifying the sanctity of the contents of communications to public group e-mail IDs. E-mail Administrator is responsible for implementing the technical controls for managing group e-mail IDs.

11.9.1 Restricted Group ID

a. The restricted group IDs shall not be included in the public directory.

b. The restricted group IDs shall be permitted for a defined duration only.

c. The restricted group IDs shall have an owner. The owner is required to manage the members of the group ID.

d. Except for the members of the restricted group ID, nobody shall be able to send any mail to this group ID.

11.9.2 Public Group ID

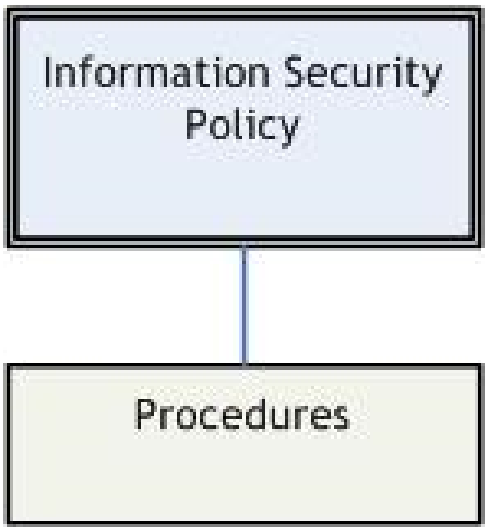
a. An approved list of e-mail IDs that can send e-mails to public group IDs shall be maintained.

b. Any user who is not part of the approved list shall not be able to send e-mail to the ‘Public’ group ID. Exception to this would be the group IDs where incident, grievances, etc. could be reported by any user.

c. An approval on the contents of e-mail shall be taken from the HR& A function/Internal Communication function prior to sending any communication to this group.

d. E-mail administrator is required to manage the addition or deletion of users in public group IDs.

12. Information Security Policy Framework



12.1. Policy

A Policy is an overall declaration of management intent for information security. It states what needs to be done to foster information security goals and objectives of Bharti Real Estate. This policy is based on the ISO 27001 Standard. It also takes into consideration generally accepted information security practices and the legal and regulatory requirements such as IT Act.

12.2. Procedures

Procedures are detailed guidelines specifying how to implement the measures defined in the standards or policies.

13 Disaster Recovery

13.1 Disaster Recovery Procedure

13.1.1 All centralized applications should have a Disaster Recovery (DR) plan. Downtime for centralized applications could result in considerable loss of business for Bharti Real Estate. All these applications should have necessary provisions for timely recovery in the event of a disaster. A disaster is defined as a sudden, unplanned calamitous event that creates an inability on the part of an organization to provide the critical business functions for some predetermined period of time and which results in great damage or loss.

13.1.2 For the purpose of DR planning, the application should be considered as a single entity which has the following components - application software, supporting network links and devices and all associated infrastructure including servers and clients required for accessing the application data.

13.1.3 Application owners will be responsible for developing disaster recovery strategy and plan for their respective applications.

Team shall ensure to conduct the DR Drill with the defined cycle from October to October every year.

13.2 Business Impact Analysis

13.2.1 Application owner should setup a DR Planning (DRP) team. DRP team should have application owner, system administrator and Information Systems Security Formulation and Implementation Team (ISSFIT) representative.

13.2.2 The DRP team will consult with business units to understand the criticality of application and acceptable down time.

□ Determine functions supported by the application

□ Determine interdependencies between these functions

□ Identify disaster scenarios and assess impact of outage

□ Determine acceptable downtime for functions

13.2.3 BIA will consider the following aspects.

□ Loss to the Business if the application fails

□ Legal and regulatory requirements.

□ Identify various possible disaster scenarios including physical damage/ destruction of servers, of Data Center, of communication links or major power outages.

□ Resources required for running the application.

□ Both the qualitative and quantitative impact of failure should be considered. Quantitative impact should estimate the monetary loss either in absolute value or percentage scale. Qualitative impact should detail out intangible losses that can impact operationally but that cannot be quantified in monetary terms.

13.2.4 DRP team should arrive at the Recovery Time Objective (RTO) based on the results of BIA. Recovery Time Objective (RTO) is the time within which business functions or application systems must be restored to acceptable levels of operational capability to minimize the impact of a disaster.

13.3 Disaster Recovery (DR) Strategy

13.3.1 The DRP team will execute the hot site strategies.

□ Alternate warm site with periodic data updation with primary site - Warm site will have all the necessary IT equipment including servers and network links. Latest data has to be restored before personnel can move in and operations can start. Typical recovery time will be more than a day.

□ Hot site - Hot site will have all the necessary IT equipment and data replication will be enabled with primary site to ensure that site is always current in terms of operational readiness. The only delay involved in starting operations is for the personnel to move in. Typical recovery time will be within a day.

13.3.2 DRP team will go ahead with hot site strategy and identify the requirements for executing the strategies.

13.3.3 DRP team should determine the recovery point objective (RPO) within the chosen strategy. RPO is defined as the point in time to which data should be recovered by DR plan. RPO will be a trade-off between the costs of lost data / cost of updating data from other sources versus cost of recovering to the most current data.

13.3.4 Based on the inputs received from DRP team, application team should take a decision on the DR strategy.

13.3.5 Head of IT should approve the DR strategy for all centralized applications.

13.4 Disaster Recovery (DR) Plan

13.4.1 Disaster recovery plan should be developed based on the strategy. DR plan should contain emergency response plan, recovery plan and restoration plan. DR plan will contain details on what steps will be taken in the event of a disaster and should be developed by DRP team with participation from select users.

13.4.2 DR plan should identify an emergency response team and clearly identify the steps to be taken in the event of disaster. Emergency response procedures are required to prevent or limit damage to IT equipment and vital business functions. This will include identifying who will be in command during this phase, who all need to be communicated, mode of communication, actions to be taken for damage mitigation, contact numbers of key personnel and emergency services, etc.

13.4.3 DR plan document should be stored securely with easy accessibility to recovery team. Approved copies of the plan should also be stored in offsite locations.

13.4.4 DRP team should identify the disaster declaration criteria based on which the DR plan should be activated. This is an important step as decision makers will be under tremendous pressure when a disaster happens. DRP team should clearly identify when a problem becomes a disaster and who will declare disaster.

13.4.5 The recovery team will be responsible for starting operations at the alternate site / alternate hardware. DR plan should detail the roles and responsibilities assigned to each person during recovery. This will involve identifying the various possible disaster scenarios and identifying detailed steps to recover for each of them. Recovery team should have detailed inventory of items that should be there in the alternate site including hardware, software, communication equipment, network diagram etc. Roles and responsibilities of each of the team members should be clearly identified. This will also include responsibilities of external vendors who will be participating in the exercise.

13.4.6 The ERT team will be involved in recovering the operations at the failed site. Restoration team should have detailed inventory of items that should be there in the original site including hardware, software, communication equipment, and network diagram. DR plan should also include the criteria for restoring operations in the primary site.

13.5 Awareness and Training Program

13.5.1 The DRP team should conduct periodic awareness and training programs for the participating teams (emergency response team, recovery team and DRP team) after the DR plan is designed. The objectives of this exercise is to

□ Communicate importance of the plan

□ Educate the team about disaster recovery provisions

□ Creating awareness about responsibilities

13.6 Testing of DR Plan

13.6.1 Test exercise should be conducted once a year by DR testing team to verify the appropriateness of the DR plans. This will create familiarity with the procedures before disaster, which will result in less confusions and faster recovery times. The main objectives of conducting periodic tests is to:

□ Verify the plan is viable and practical

□ Verify that recovery time frames can be met

□ Rehearse and train all personnel involved in recovery

□ Eliminate errors and omissions in the plan

□ Update the plan in the light of the results

13.6.2 Specific set of users who are involved in disaster recovery should participate in the testing program. The DR testing team should also decide the type of testing program. One of the following methods or a combination of these can be used for testing.

□ Structured Walk-Through - Users involved in DR recovery Team members meet to verbally walk through each steps of the plan to confirm the plan effectiveness and identify gaps, bottlenecks and other plan weaknesses.

□ Simulation test - This involves the development and use of a pre-written test scenarios or test scripts for disaster events. The scenarios tell the team members how to react to such disasters and give organizations a baseline from which to start their recovery plans.

□ Mock disaster test - This is full-fledged disaster recovery plan test. The purpose is to test as many components of the disaster recovery plan as possible. The test is likely to be costly and could disrupt normal operations and therefore should be approached with caution and prior approval of concerned department head/branch manager.

13.6.3 The DR testing team should decide the schedules and frequencies of conducting the testing program.

□ Schedule for conducting a test once a year after the plan is designed.

□ Schedule once a year testing so that personnel are aware of their responsibilities in case of role changes within the organization. Testing should also be conducted soon after any major review and change in DR plan.

13.6.4 The DRP team should evaluate the DR plan based on the test results. Expected results should be compared against actual results. The DR plan can be updated based on the evaluation.

13.7 Review of DR Plan

13.7.1 Application owner should be responsible for reviewing and updating the DR strategy and DR plan.

□ DR strategy should be reviewed if there is any major change in business or IT infrastructure.

□ DR plan should be updated whenever there is a change in DR strategy.

□ DR plan should be updated frequently to reflect changes in personnel assigned with roles under the plan. All contact details identified in the plan should be verified periodically.

14. Internet Usage Policy

14. 1. Objective

An internet usage policy provides user with rules and guidelines about the appropriate use of company equipment, network and Internet access.

Having such a policy in place helps to protect both the business and the employee; the employee will be aware that browsing certain sites or downloading files is prohibited and that the policy must be adhered to or there could be serious repercussions, thus leading to fewer security risks for the business as a result of employee negligence.

14.2 Unacceptable use of the internet by the Employee/Associate, but is not limited to:

- Sending or posting discriminatory, harassing, or threatening messages or images on the Internet or via Bharti Real Estate email service

- Using computers to perpetrate any form of fraud, and/or software, film or music piracy.

- Stealing, using, or disclosing someone else's password without authorization
- Downloading, copying or pirating software and electronic files that are copyrighted or without authorization.
- Sharing confidential material, trade secrets, or proprietary information outside of the organization
- Hacking into unauthorized websites
- Sending or posting information that is defamatory to the company, its products/services, colleagues and/or customers.
- Introducing malicious software onto the company network and/or jeopardizing the security of the organization's electronic communications systems
- Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities.
- Passing off personal views as representing those of the organization

All terms and conditions as stated in this document are applicable to all users of Bharti Real Estate network and Internet connection. All terms and conditions as stated in this document reflect an agreement of all parties and should be governed and interpreted in accordance with the policies and procedures mentioned above. Any user violating these policies is subject to disciplinary actions deemed appropriate by Bharti Real Estate.

14.3 Internet Access for Guest users.

For extended the internet access to the guest of Bharti Real Estate for business user. Following procedure is required to be followed.

1. Request form (Annexure 1) should be duly filled and approved from the requester and department head.

2. IT helpdesk to extend the internet access post Mac binding procedures.

14.4 Annexure 1

Exception Request Form

Internet Access\WIFI Access\ Printer Access

bharti
Bharti Realty Limited
(A Bharti Enterprise)

Section1: Exception Details

Requestor Name **Emp. ID** **Email ID** **User ID (filled by IT)** **Computer Name\MAC** **Company Name**	
Exception Type - **Internet (Description of URL)** - **Printer Access\Printer Name** - **Local Administrative (Privilège ID) Access**	□ □ □
Business Justification	
Exception required up to Date **(DD/MM/YYYY)**	
Requestor's Location Name	
Requestor's Function Name	

Section2: Requestor and Approver's Name & Signature

Requestor Name & Signature:	**Functional - Head / Reporting Manager of Bharti Real Estate Name & Signature:**	**IT Manager / IT Head Name & Signature (confirm non-availability of any secure workaround):**

Bharti Real Estate Confidential:

- **Unauthorised access is not allowed.**
- **Password and ID sharing not allowed**