Bharti Airtel Information Security Policy / Africa

Version 1.0

Document Control

S. No.	Type of Information	Document Data
1.	Document Title	Bharti Airtel Information Security Policy/Africa
2.	Document Code	BISP/Africa/Africa
3.	Date of Release	01/09/2011
4.	Document Superseded	
5.	Document Revision No	1.0
6.	Document Owner	Felix Mohan, Chief Information Security Officer (felix.mohan@airtel.in)
7.	Document Author(s)	Charanjit Singh Sodhi (charanjit.sodhi@in.airtel.com) Aman Nugyal (aman.nugyal@in.airtel.com) Pradeep Eledath (pradeep.eledath@in.airtel.com) Jacxine Fernandez (jacxine.fernandez@airtel.com)

Document Change Approvals

Version No.	Revision Date	Nature of Change
1.0	01 Sep 2011	Initial Release

I) Document Distribution

The Global CISO is responsible for communicating the latest version of Bharti Airtel Information Security Policy (BISP/Africa) to all the functions and geographies. The HR and SCM functions in each OpCo shall ensure distribution of the BISP/Africa to all employees and the relevant third parties respectively.

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
- Annexure I – Glossary
- Annexure II – Reference Mapping of Procedures and Standards with the BISP/Africa 1.0 Controls

Annexure I and Annexure II are separate documents.

Index

1. Information Security Policy (BISP/Africa – 001)

1.1. Introduction

It is the policy of Bharti Airtel International Netherlands BV, hereinafter referred to in this document as "airtel", that its information assets are provided comprehensive protection against the consequences of breaches of confidentiality, failures of integrity and/ or interruptions to their availability. The Bharti Airtel Information Security Policy/Africa (hereinafter referred to as BISP/Africa in this document) provides management direction and support to implement information security across airtel.

1.1.1 Scope

The BISP/Africa is applicable to all information assets of airtel. 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 BISP/Africa is applicable to all employees and third parties of airtel.

As a reference for this document, a service provider is called a Third-party only after association with airtel. These third parties are strategic partners who enter into direct contracts with airtel 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 airtel. Third parties include IT service providers, telecommunication service providers, call-centre vendors, value added service providers (VAS, VAS O&M), payment gateway vendors, 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 airtel.

The BISP/Africa is applicable across all business units of airtel. The BISP/Africa is applicable across all geographies where the information assets of airtel are located.

1.1.2 Policy Owner

The owner of the BISP/Africa is the Global Chief Information Security Officer (hereinafter referred to as Global CISO in this document). The Global CISO shall be responsible for maintaining and updating of the BISP/Africa 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 BISP/Africa and any subsequent modifications to the BISP/Africa.

Global Chief Information Security Officer (Global CISO): The Global CISO, as defined in the *section 2.3.2* of this document, shall be responsible for ensuring that policies constituting the BISP/Africa are current and reflect the requirements of airtel.

Information Security Working Group (ISWG): The ISWG, as defined in the *section 2.3.3* of this document, shall be responsible for enforcing the implementation of relevant BISP/Africa clauses as per the *Bharti Airtel Functional Check-Off List of BISP/Africa Clauses*. The accountability for this shall remain with the ISSC members.

All Employees: It is the responsibility of all employees and third party staff to read, understand and adhere to the BISP/Africa.

1.2. Policy Statement and Objective

Security of information assets of airtel 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 BISP/Africa provides management directive for information security and recommends appropriate security controls that need to be implemented to maintain and manage the information security in airtel. airtel shall strive to secure information by:-

a. Establishing and organising an Information Security Governance Framework;

b. Developing and maintaining an effective Information Security Management System (hereinafter referred to as ISMS in this document) consisting of an Information Security Policy document, supporting Procedures and a Risk Management Framework;

c. Ensuring that the policies and related procedures are designed in such a way that they can align themselves to the Enterprise Risk Management Framework;

d. Ensuring that the information security posture of airtel keeps pace with the cultural maturity of the organisation over the following stages: from ad-hoc to vulnerability driven; from vulnerability driven to risk driven; from risk driven to enterprise driven;

e. Deploying appropriate technology, resources and infrastructure;

f. Constantly monitoring, reviewing, exception-reporting and taking actions thereon for improving the effectiveness of the ISMS;

g. Taking appropriate actions for any violations of the BISP/Africa; and

h. Creating and maintaining a security-conscious culture in airtel.

1.3. Review and Evaluation

The BISP/Africa 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 BISP/Africa document shall be reviewed by the Global CISO 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 BISP/Africa 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 BISP/Africa.

b. Non-compliance with the BISP/Africa is ground for consequence management, up to and including termination. The relevant HR process shall be invoked for Consequence Management.

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 BISP/Africa is intended to be a statement of information security requirements that need to be met in airtel. However, exceptions against individual controls in specific policy domains shall be formally documented in the Security Override Document (hereinafter referred to as the SOD), which will include, at a minimum, the following:-

a. Justification for the exception;

b. Risk due to the exception;

c. The mitigation controls to manage the risk;

d. The plan of action to manage the risk; and

e. The validity period of the exception.

The exception request, validation and management shall be done as per the *Exception Management Procedure.*

2. Information Security Organisation Policy (BISP/Africa – 002)

2.1. Introduction

The *Information Security Organisation Policy* defines appropriate responsibilities, authority and relationships to manage information security in all business functions. The information security organisation has representation from all 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 Global CISO to manage the information security organisation within airtel.

2.2. Policy Statement and Objective

An information security organisation shall be set up to undertake information security activities in accordance with the BISP/Africa in all business functions.

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

a. An ISMS 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. 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 of the Airtel International Management Board:-

	Names	***Title***	***Email address***
1	Manoj Kohli	CEO and JMD International	manoj.kholi@airtel.com
2	Bhaskar Chakraborty	Chief Supply chain Officer	bhaskar.chakraborty@airtel.com
3	N. Arjun	Projects Management	n.arjun@airtel.com
4	Rupinder Goel	Chief IT Officer	rupinder.goel@airtel.com
5	Rahul Gupta	Chief Customer Service Officer	rahul.gupta@airtel.com
6	Hans Van Lierop	Chief Finance Officer	hans.vanlierop@airtel.com
7	Yves Mayilamene	Chief HR Officer	yves.mayilamene@airtel.com
8	Stephen Torode	Chief Strategy Business Development Officer	stephen.torode@airtel.com
9	Tiemoko Coulibaly	CEO - Francophone	tiemoko.coulibaly@airtel.com
10	Andre Beyers	Chief Marketing Officer	andre.beyers@airtel.com
11	Jayant Khosla	CEO - Anglophone	jayant.khosla@airtel.com
12	Rajan Swaroop	CEO - Nigeria	rajan.swaroop@ng.airtel.com
13	Kim Lee Tay	Director - Internal Audit	kimlee.tay@airtel.com
14	Eben Albertyn	Chief Technical Officer	eben.albertyn@airtel.com

The ISSC shall meet at regular intervals, at least once in a quarter. The ISSC shall have the following responsibilities:-

a. Ensuring the establishment of the ISMS objectives and plans;

b. Approving the BISP/Africa;

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

d. Communicating the information security plans and programs to maintain information security awareness in airtel;

e. Conducting management reviews of the ISMS; and

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

2.3.2 Global Chief Information Security Officer (Global CISO)

The Global CISO is responsible for the establishment and maintenance of the ISMS. The Global CISO shall have the following responsibilities:-

a. Identifying information security objectives and strategizing them consistent with the corporate strategic plans;

b. Managing the development and implementation of the BISP/Africa and its procedures to ensure on-going maintenance of information security;

a. Overseeing security operations, including information security incident management and business continuity management;

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

c. The Global CISO could issue 'special instructions' in emergent cases required for carrying out investigations and forensics. Such special instructions would be issued by the Global CISO 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;

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

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

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

2.3.3 Information Security Working Group (ISWG)

Every Operating Company (OpCo) shall have an ISWG consisting of the following: -

a. Information Technology;

b. Human Resources;

c. Legal and Regulatory;

d. Finance;

e. Marketing and Sales;

f. Networks;

g. Customer Service Delivery;

h. Supply Chain Management; and

i. Corporate Audit Group (as Observer).

The ISWG shall meet at regular intervals, at least once in a quarter. Members of the ISWG shall have an explicitly stated Key Result Area (KRA) for performance of their security responsibilities.

The ISWG shall be responsible for the following:-

a. Acting as representatives of their respective functional directors on all information security related issues pertaining to their individual functions;

b. Implementing, within their respective functions, the relevant information security requirements as defined in the *Functional Check-Off List of BISP/Africa Clauses*. The check-off list provides a list of BISP/Africa clauses that each function must implement;

c. Developing and owning their respective 'Functional Security Plans' (FSP). The FSP shall provide information on how the requirements specified in the *Functional Check-off List of BISP/Africa Clauses* would be implemented by their functions across the organisation. The ISWG members shall get their FSPs approved by their respective functional directors;

d. Keeping their respective FSPs updated in line with any new development or change in their respective functional domains that could impact the delivery of the functional security requirements within their functions;

e. Resolving any inter-functional issues that may arise while delivering the functional information security requirements across the organisation; and

f. Assisting in periodic updating of the *Functional Check-Off List of BISP/Africa Clauses* with regard to the controls relevant to their respective functional domains, as required.

2.3.4 OpCo Functional Security SPOC

Each member of the Executive Council at the OpCo shall function as the OpCo Functional Security Single Point of Contact (SPOC) for his/her respective function. The OpCo Functional Security SPOC shall be responsible for implementation of the relevant information security requirements as defined in the *Functional Check-off List of BISP/Africa Clauses* applicable to their respective functions.

The OpCo Functional Security SPOCs shall, in addition to implementation of the BISP/Africa functional check-off list clauses applicable to their respective functions, also be responsible for:-

a. Ensuring that the BISP/Africa and related procedures are implemented within their functions in the OpCo;

b. Preparing and keeping up-to-date their respective Functional Asset Registers and ensuring that the Asset Register is in accordance with the *Asset Management Policy (Refer to BISP/Africa-003)*;

c. Coordinating during the Risk Assessment and Internal Audits;

d. Carrying out root cause analysis, including the investigations, for the reported security incidents and proactively identifying security weaknesses and incidents.

2.3.5 OpCo Information Security Team (OIST)

Each circle shall have an OpCo Information Security Team (OIST). The OIST shall be chaired by the Head of the Executive Council at the OpCo, i.e. the CEO/COO/MD. All the Executive Council members shall be the members of the OIST and shall function as the OpCo Business Continuity Team.

The OIST shall be responsible for the following:-

a. Overseeing all aspects related to security operations and driving overall information security in the OpCo;

b. Overseeing information security incident response planning, preparedness, and response;

c. Conducting the Investigation of security breaches;

d. Recommending disciplinary measures as part of circle consequence management process to ensure that employees, partners, and third parties comply with requirements of BISP/Africa and Bharti Airtel Third-party Security Policy (BTSP);

e. Managing and implementation of information security training and awareness programmes;

f. Resolving cross-functional information security issues in business processes that extend across more than one function;

g. Facilitating conduct of Internal and External Audit;

h. Preparation and maintenance of OpCo-level asset and risk register; and

i. Business continuity management, including testing of the Business Continuity Plan.

The Chairperson of the OIST and each of the OpCo Functional Security SPOCs shall have an explicitly stated KRA for performance of their security responsibilities.

2.3.6 Allocation of Information Security Responsibilities

All function heads of each OpCo shall ensure that the information security responsibilities of employees in their functions are identified, documented and communicated to them.

2.3.7 Authorisation Process for Information Processing Facilities

All new information processing facilities shall be set up only after receiving the necessary approvals within airtel. No personal computing/storage devices, such as laptops, USB pen drives, external hard disk drives, data cards, modems, mobile phones as modem (GPRS), etc. shall be physically or logically connected to airtel's network or to any information asset of airtel.

2.3.8 Contact with Authorities

Contacts with law enforcement authorities, fire department, emergency services and telecommunication providers 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.

2.3.9 Contact with Special Interest Group

The Global CISO shall maintain appropriate contact with special interest groups and authorised information security forums for receiving and distributing the updates on new vulnerabilities, security threats, regulations and/ or risks pertaining to the telecom industry and to the services that are provided by airtel.

2.4. Third-party Security

a. All third parties are required to adhere to the *Bharti Airtel Third-party Security Policy* (BTSP). If the third parties sub-contract any service/work pertaining to airtel, the sub-contracted parties and their employees are also required to adhere to the BTSP.

b. In accordance with the BTSP, all Third-parties are required to submit specified documents such as the Pre-Association Checklist, RFP Template, Legal Agreement, etc. pertaining to information security prior to any engagement.

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

2.4.1 Identification of Risk Related to Third-party Access

The IT/ Networks function is required to carry out a risk assessment to identify the information security implications and the asset owner has to accept the identified risk. 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 airtel and the third party only for what is explicitly required for information exchange. Everything else shall be denied; and

c. Clearance from the airtel Africa Security Team is obtained before providing any access to third parties.

3. Asset Management Policy (BISP/Africa – 003)

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 ratings of the assets. 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 of each OpCo 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, labelling and ensuring the protection of their respective information assets as per the *Asset Management Procedure*. The asset owner is also responsible for identifying the asset custodians for the assets under his/ her ownership.

The asset custodians are responsible for the implementation of the required controls for the protection of information assets.

All employees and third party staff are responsible for handling information assets as per the classification of the asset.

3.2. Policy Statement and Objective

Information assets of airtel shall receive comprehensive protection and shall have an identified owner.

The objectives of the policy are to ensure that:-

a. An information asset register documenting the 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. The CIA (Confidentiality, Integrity and Availability) ratings of information assets are ascertained.

3.3. Asset Register

The asset register documents the information assets of a business function. All business functions are required to maintain an asset register of their business function as per the *Asset Management Procedure.* The asset register is required to contain, at a minimum, the following information about the assets:-

a. The type and location of assets;

b. Name of the function and process that uses this asset;

c. The Asset Owner, Custodian and User;

d. The CIA ratings of the asset, etc.

3.4. 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.

3.4.1 Ownership of Assets

The head of each business function is required to ensure that his/ her function's information assets have identified and documented asset owners. The asset owners shall be responsible for the appropriate classification of the asset as per the *Asset Management Procedure* and shall ensure that the security controls required to protect the assets are implemented.

3.5. 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 with the business requirement and takes into account 'Confidentiality', 'Integrity' and 'Availability' ratings of the information.

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

a. Strictly Confidential

This classification applies to the most critical business information, which is intended strictly for use within airtel. Its unauthorised disclosure could adversely impact its business, its shareholders, its business partners and/ or its customers, leading to legal and financial repercussions and adverse public opinion.

b. Confidential

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

c. Public

This classification applies to information, which has been explicitly approved by the management for release to the public.

d. Internal

This classification applies to information that is specifically meant for employees of airtel. 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.

For information that is classified as 'Strictly Confidential' or 'Confidential', an assessment shall be done to identify the business, legal and/ or regulatory requirements for ascertaining its expected retention period. It is recommended to refer to the *Information Classification Standards* document for more details about the aforesaid classifications.

3.5.1 Information Labelling and Handling

All important tangible assets shall be labelled physically as per the *Information Labelling and Handling Procedure*. The asset owners are required to ensure that their assets are appropriately labelled (marked) for ease of identification. This may exclude information classified as 'Public'. For each classification level, the handling including its secure processing, storage, transmission and destruction have been defined in the *Information Labelling and Handling Procedure*.

3.6. Temporary Asset Acquisition, Maintenance and Release Policy

Temporary assets shall be appropriately managed and provided comprehensive protection during their life-cycle in airtel. The primary intention of this policy is to establish secure and reliable acquisition, maintenance and release of temporary assets at airtel.

3.6.1 Temporary Asset

A temporary asset is defined as "An asset which is put to use in airtel for a temporary period of time, but is not a property of airtel." The organisation shall use these assets under a contract with the Third Party that provides these assets. The temporary asset could be on hire and used for a specified period of time such as used for conduct of proof of concepts, trials, etc. A temporary asset could include, but is not limited to, computer equipment (desktops, servers, processors, monitors, laptops, modems, printers, etc.), communication equipment (network devices, PABX, fax machines, etc.), magnetic media (tapes, disks, CDs etc.), AV equipment (data projectors, plasma screens, LCD monitors, audio equipment, TVs, DVDs, VCRs, sound systems, staging and lighting, video and conference equipment, etc.), communication devices (PDA, mobile phones, etc.), software assets (software products, development tools, utilities, etc.) and so on.

These assets shall be maintained and managed as per the *Temporary Asset Acquisition, Maintenance and Release Procedure*. The procedure shall include the following:-

a. Secure entry and exit of temporary assets;

b. Maintenance of temporary information asset registers;

c. Secure environment check for information assets prior to connecting them to the IT or Network infrastructure; and

d. Secure and timely return of the temporary asset to the Third Party, if required, after the sanitisation of the information stored in any information asset.

4. Human Resources Security Policy (BISP/Africa - 004)

4.1. Introduction

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

4.1.1 Responsibility

The Human Resources (HR) function is responsible for the implementation and maintenance of the controls defined in the *Human Resources Security Policy*.

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

All employees and third party staff are required to understand and adhere to their information security responsibilities during and after their employment/ tenure with airtel.

4.2. Policy Statement and Objective

Information security controls shall be designed and integrated in the HR processes to ensure that employees and third party staff understand their responsibilities and are suitable for the roles they are considered for and to reduce the risk of theft, fraud or misuse of information assets.

The objectives of this policy are to:-

a. Ensure that the employees and third party staff understand their responsibilities and roles regarding information security;

b. Reduce the risks due to human error, theft, fraud or misuse of information assets and facilities; and

c. Minimise the damage from the security incidents and malfunctions and learn from such incidents.

Failure to adhere to information security responsibilities may result in appropriate actions through the consequence management process.

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. These security responsibilities shall be reflected in the Job Descriptions and the Terms and Conditions of Employment. The HR function shall conduct background verification checks for employees in accordance with the relevant HR policy.

4.3.1 Roles and Responsibilities

The HR function shall ensure the following:-

a. The security roles and responsibilities of employees are defined and documented in their Job Descriptions (JD) in accordance with the BISP/Africa;

b. The roles and responsibilities include reporting of the potential security weaknesses and incidents;

c. The security roles and responsibilities are clearly communicated to every new employee during the induction process and also through sessions whenever there is any change in the policy; and

d. Performance of information security responsibilities is defined and measured as Key Result Areas (KRA) of employees.

4.3.2 Screening

a. It is recommended that the HR function carries out background verification checks of prospective employees for employment as per the relevant HR policy.

b. The background verification checks process should ensure that all personal information is kept confidential and the privacy of the prospective employee's data is maintained.

c. The contract with the background verification agency, if any, shall clearly specify the agency's responsibilities for verification.

d. The third parties are required to carry out background verification checks of their employees who have access to information assets of airtel and provide a certificate to this effect to the HR function of airtel.

4.3.3 Terms and Conditions of Employment

The HR function is required to ensure that the Terms and Conditions of Employment reflect the information security requirements and include the following:-

a. The requirement for all employees to sign a confidentiality agreement which will hold them liable for any unauthorised disclosure, modification and/ or destruction of information;

b. The responsibility for maintaining the confidentiality and integrity of information;

c. The actions to be taken, if any user disregards the requirements of the BISP/Africa; and

d. The continuation of the employee's responsibilities for protecting the confidentiality of the information of airtel even after termination of employment.

4.4. During Employment

HR function is required to take appropriate actions to ensure that:-

a. The employees are made aware of their security responsibilities to maintain information security; and

b. An adequate level of awareness, education and training on information security is provided to all employees.

4.4.1 Code of Conduct and Non-Disclosure Agreement

a. All employees are required to do the following:-

   i. Sign the Code of Conduct at the time of joining the organisation and once in every subsequent financial year thereafter; and

   ii. Sign the acceptance of the BISP/Africa at the time of joining and once in every subsequent financial year thereafter.

b. All third party staff who access/ manage the information assets of airtel are required to do the following:-

   i. Sign a Non-disclosure Agreement (NDA); and

   ii. Sign the acceptance of the *Third Party Security Policy* at the beginning of their tenure with airtel and every subsequent year thereafter.

4.4.2 Management Responsibilities

The ISWG in each OpCo shall ensure that importance of information security is communicated to all employees to maintain an information security conscious culture in airtel.

4.4.3 Information Security Awareness, Educating and Training

The HOD of each function in each OpCo shall ensure that every employee of his/her function attends information security training workshops, whenever these are conducted.

The HR function shall ensure that:-

a. Formal Information Security Training is imparted to the employees at the time of their induction and at least once in every six months thereafter;

b. The training programme includes the relevant sections of BISP/Africa with appropriate Dos and Don'ts that the employees need to practise in their day-to-day work; and

c. Half Yearly Certificates is awarded to employees who successfully complete such training.

4.4.4 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 sirt@cc.airtel.com. Here "cc" represents the "country code" of each OpCo.

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.

4.4.5 Disciplinary Process

a. Certain categories of activities, which have the potential, or actually harm the information assets are defined as security violations and are strictly prohibited. Such security violations shall result in the invocation of the consequence management process.

b. The HR function and functional heads dealing with third parties shall ensure that employees and third parties are made aware of the formal disciplinary process which may be initiated against them, if they violate the BISP/Africa or BTSP or commit/ participate in any kind of security breach. The formal disciplinary process shall take into account factors such as nature and gravity of the breach, its impact on perpetrator and relevant laws.

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, parking stickers, manual and/ or any other asset that is the property of airtel.

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 and Networks 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 and Networks 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 and Networks 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.

5. Physical and Environmental Security Policy (BISP/Africa – 005)

5.1. Introduction

The *Physical and Environmental Security Policy* provides direction 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 of controls defined in the *Physical and Environmental Security Policy*. The IT and Networks functions, however, are required to support the Administration function for the implementation and maintenance of physical and environmental security controls as specified in this policy.

5.2. Policy Statement and Objective

airtel 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. 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 function is required to define the physical security perimeter for all office locations, facilities and the geographies where information assets of airtel 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. Information Security shall be integrated with physical security through integration of systems such as access control systems, intrusion protection systems, video surveillance system, etc.

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

c. All premises and facilities, where information assets of airtel are hosted, shall be classified into zones as per the *Physical Zoning Standards*.

d. The *Physical Zoning Standards* shall provide the classification criteria and security controls for areas like Data Centres, Reception Areas and Internal office areas.

e. The security controls defined in the *Physical Zoning Standards* shall be implemented in all classified zones.

5.3.3 Securing Offices, Rooms and Facilities

a. All facilities shall remain secured during and after office hours or when unattended.

b. Appropriate level of security controls shall be implemented to prevent unauthorised access in office areas and facilities hosting critical equipment.

5.3.4 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, Development Centres, etc. The administration function with the assistance of IT and Networks functions are 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, as specified in *Physical Zoning Standards*, are 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 and recorded as far as possible; and

d. Photographic, video, audio or other recording equipment, such as cameras in mobile devices shall not be allowed in secure areas. Sufficient arrangements for depositing these devices to the security guard at the entry point of secure areas shall be made. The employee responsible for the physical security of the secure area shall ensure this. A list of equipment/ devices that are not allowed inside these areas shall be displayed at the entry point.

5.3.5 Public Access, Delivery and Loading Areas

a. It shall be ensured that all areas, where loading and unloading of items are done, are monitored and equipped with the appropriate physical security controls during these activities.

b. Access to these areas shall be confined to authorised personnel only during these activities.

c. The movement of all incoming and outgoing items shall be documented and incoming items shall be inspected for potential threats.

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 and humidity control systems to support information systems and equipment;

b. Implementation of flood protection measures;

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

d. Implementation of adequate power supply controls to ensure continuous power supply; and

e. Creation and implementation of emergency evacuation plans including the formation of an Emergency Response Team (ERT) to ensure emergency evacuation.

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

All equipment shall be protected against environmental threats and unauthorised access. IT/ Networks 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;

e. A preventive maintenance exercise for the utility equipment is carried out at scheduled intervals ensuring their continued availability and integrity; and

f. A review of preventive maintenance is conducted by the HOD of Administration function.

5.5.3 Cabling Security

a. All cables, including power and telecommunication network cables, shall be protected from damage or unauthorised interception.

b. All network cables and their corresponding terminals shall be identified and marked.

c. Documents, including the detailed physical network diagrams, showing cable routings and terminations shall be held by the Head of Administration Function or his designated personnel.

d. As far as possible, power cables shall be segregated from communication cables.

5.5.4 Security of Equipment Off-premises

The IT, Networks and Administration functions are required to apply appropriate security controls to off-site equipment considering the various risks that may exist outside the premises. Portable equipment such as Laptops, Blackberry, etc. that are owned by airtel shall be covered under insurance. It shall be ensured that:-

a. All equipment (such as telecom switches, Base Transceiver System (BTS), distribution points, backup media, etc.) receive an appropriate level of protection against physical and environmental threats; and

b. Equipment installed outside the organisation premises are monitored at specified intervals.

All employees are required to ensure that if equipment and/or media need to be taken outside the organisation's premises, it is done in accordance with the *Security of Equipment Off-premises Procedure*.

5.5.5 Secure Disposal and Re-use of Equipment

a. Employees and third party staff are required to ensure that information systems of airtel are disposed of only after obtaining approval from authorised personnel. The *Media Disposal Procedure* shall be followed for secure disposal of media. Sensitive data and licensed software shall be removed from the media prior to its disposal.

b. The procedure for secure disposal of media would apply to all devices owned by airtel and also to the disposal of storage media (such as Hard Disk Drives) in machines (such as laptops) that are hired by airtel.

c. All storage media that needs to be disposed of shall be degaussed prior to disposal. The storage media that is degaussed shall not be reused.

d. If it is possible to "definitely state" that there is (a) NIL sensitive data in a storage media and (b) The storage media is being transferred within airtel, then software overwrite can be used to clean the storage media, instead of degaussing. The secure overwrite should be done by a tool that meets the specification of "DOD Secure Overwrite".

e. The process for accounting of removed storage media, storing it securely till degaussed, and then following a secure process for disposing the degaussed storage media shall be implemented.

5.5.6 Removal of Property

The HODs of all functions are to ensure that all utility equipment, information systems, storage devices and/or software of airtel are removed from the premises of airtel with proper authorisation in accordance with the *Removal of Property Procedure*.

6. Communication and Operations Management Policy (BISP/Africa – 006)

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 Operations – Service Delivery team is responsible for the implementation of controls defined in this policy in the IT infrastructure.

The Networks function is responsible for the implementation of controls defined in this policy in the telecom infrastructure.

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

The HOD of both IT and Networks functions are responsible for enforcing the implementation of this policy in their respective functions.

6.2. Policy Statement and Objective

airtel 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. Identify and develop documented operation procedures for information systems and computing devices;

b. Ensure protection of information during its transmission through communication networks;

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

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

e. Maintain security during information exchange with the other organisations.

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

   vii. Any maintenance/ support agreements with the details of the contact names and commencement and termination dates of agreements.

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 airtel 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.

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.

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 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.

e. All test data, temporary accounts and temporary passwords shall be removed from the systems prior to deploying them into the production environment.

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 BISP/Africa 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 and Networks functions shall establish a process to ensure the following:-

a. Services, reports and evidences 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 BISP/Africa 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 and Networks functions in consultation with the following:-

   i. Asset owners of the existing systems; and

   ii. Heads of departments requiring the new system.

b. Capacity planning shall specifically provide for capacity enhancements required for security-related logging, analysis and exception-reporting.

c. 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 airtel Africa Security Team before any new information systems, upgrades and/or new versions are accepted.

6.6. Protection against Malicious and Mobile Code[1]

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.

e. The 'auto run' feature shall be disabled on all systems.

[1] Mobile code is software obtained from remote systems, transferred across a network, and then downloaded and executed on a local system without explicit installation or execution by the recipient. Examples of mobile code include scripts (JavaScript, VBScript), Java applets, ActiveX controls, Flash animators, Shockwave movies.

6.6.2 Controls Against Mobile Code

a. In the information systems where the use of mobile code is authorised, the configuration of the system shall ensure that only authorised mobile code operates according to a clearly defined set of rules.

b. Appropriate safeguards shall be implemented in the information systems to prevent the execution of unauthorised mobile code.

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 and Networks 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 and Networks 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 logs are to be maintained;

   iv. Maintenance and preservation of backup logs;

   v. Legal, regulatory and contractual requirements, as applicable;

   vi. Storage of backup media; and

   vii. 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. Frequency of backup and restoration testing shall reflect the business requirements.

e. Backup operators are responsible for the appropriate rotation of backup media. The rotation schedule and the number of tapes shall be decided on the basis of business requirement of backed up data.

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

g. Business-critical data shall be duplicated. One copy shall remain onsite and the other stored in a secured off-site location. The backup media shall be kept in fireproof safe.

h. Backup media shall be handled in accordance with the classification of the data stored on it and shall be disposed of as per the Media Disposal Procedure.

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

j. Reliable and secure transport shall be used when transporting backup media to an off-site location.

6.8. Network Security Management

6.8.1 Network Controls

Controls shall be implemented by IT and Networks functions to protect the airtel network. The network controls shall ensure that the network documentation is maintained including document control history. Suitable information security controls shall be implemented in the infrastructure and systems where airtel provides hosting services.

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. Partners for IT and Networks shall strictly comply with *LAN Zoning and Data Traffic Flow Guidelines*, ensuring, within their respective domains, creation of necessary zones and enforcement of all security controls to comply with these guidelines;

c. Protection of critical networks/ information systems/ applications through firewalls and NIPS's against both external and internal users. The firewall shall be configured and managed to limit access only to authorised users;

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

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

f. 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*:-

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 strong 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.

6.8.3 Firewall

Firewalls shall be deployed to limit the ingress and egress traffic in airtel network. *Firewall Management Procedure* shall be created, documented and implemented in all firewalls owned, rented, leased, or otherwise controlled by airtel. The *Firewall Management Procedure* shall include the following:-

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 and approved 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. Quarterly review of the firewall and router rule base;

g. 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 by the firewall administrator;

h. The firewall log reports, which shall be produced in a defined format, shall be reviewed by Security SPOC of IT/Network function at specified intervals;

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

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

6.8.4 Security of Network Services

a. The IT and Networks 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 and Networks 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/ Networks functions prior to the implementation of change in the production environment.

6.8.5 New Device Commissioning

a. IT and Networks functions are required to create secure configuration documents (SCD) for each kind of operating systems (Windows, Solaris, Linux, HP-UX, IBM-AIX etc.), network devices such as routers, switches and security devices such as firewall, IDS/ IPS or any other device or telecom equipment being used in the network. These SCDs shall be used for commissioning a new server, workstation, network and security devices.

b. The SCD shall be updated at defined intervals to ensure the inclusion of appropriate controls to address the latest vulnerabilities and/ or threats in the environment.

c. The creation of SCD could be excluded for the core telecom equipment; however, their exclusion shall be guided by the fact that the O/S software is embedded, pre-hardened, service specific and that these O/S are not exposed to public and have no vulnerabilities/ exploits available to public in general. Such claims shall be duly supported with the submission of a certificate by the vendor supplying the equipment to airtel giving all the necessary details.

6.9. Media Handling

6.9.1 Management of Removable Media[2]

a. All employees and third party staff are required to follow the Removable Media Management Procedure. The procedure shall include the use, storage, availability, registration, authorisation and disposal of removable media.

6.9.2 Disposal of Media

a. Media containing critical and sensitive information shall be disposed of in a secure manner.

b. The Media Disposal Procedure shall be followed for secure and safe disposal of the removal media. The technique used shall depend on the type of media and the classification of information that is contained in the media.

c. Disposal shall be done only by authorised users and a formal report of the secure disposal of media containing confidential information shall be generated and recorded.

d. All employees and third party staff are required to follow the *Media Disposal Procedure*.

6.9.3 Security of System Documentation

a. The appropriate security measures shall be implemented by the IT and Networks functions to maintain the security of the system documentation for critical information systems.

b. All system documentation shall be classified as per the *Asset Management Policy (BISP/Africa-003)*.

c. Access to these documents shall be shall be monitored, logged and reviewed.

6.10. Exchange of Information

6.10.1 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.

[2] Removable Media includes official laptops, USB pen drives, external hard disk drives, data card, modem, etc.

6.10.2 Exchange Agreements

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

6.10.3 Physical Media in Transit

a. Documents and removable media carrying information of Strictly Confidential or Confidential classification shall be transported between sites using only the services of an authorised courier agency.

b. The courier agency involved in the transport is required to sign a Non-disclosure Agreement.

c. All employees and third party staff carrying media are required to ensure its appropriate protection during transit.

6.11. Electronic and Mobile Commerce Services

6.11.1 Electronic and Mobile Commerce

Electronic commerce and Mobile commerce is collectively termed as *Digital Commerce* in this document. All information and transactions related to digital commerce undertaken by airtel shall be protected from any fraudulent activity, contract dispute, unauthorised disclosure, and modification and/ or destruction by using appropriate information security controls as follows:-

a. Appropriate authentication mechanisms, such as Verified by Visa, MasterCard Securecode etc. based on the 3D (3 Domain) Secure Protocol, shall be implemented to authenticate the identity of customers prior to authorising online transactions;

b. All online transactions shall include a mechanism for routing customer details through an online-fraud mitigation application or service, which would return a risk rating score. Authorisation for the transaction should be based on the returned risk score;

c. An online-fraud mitigation organisation would be established within the Line of Business (LOB) responsible for the digital commerce initiative. This online-fraud mitigation organisation is required to pay special emphasis on protecting digital commerce transactions against chargeback liabilities by framing appropriate fraud protection business rules in consultation with the LOB and CSD;

d. Prior to the online transaction, it shall be ensured that trading partners are fully informed on their authorisations;

e. The confidentiality and integrity of transactions are maintained by implementing a secure channel; and

f. All data of customers, including their privacy, shall be protected in accordance with applicable industry, regulatory and legislative directives in force.

6.11.2 On-Line Transactions

a. Information involved in online transactions shall be protected to prevent incomplete transmission, misrouting, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay.

b. A secure communications channel shall be setup between all involved parties for online transactions.

6.11.3 Publicly Available Systems

Adequate security controls shall be put in place to ensure the confidentiality, integrity and availability of the information contained in the publicly available systems of airtel. Prior to deployment, all publicly available systems shall be tested against for vulnerabilities and it shall be ensured that the identified vulnerabilities are fixed prior to publishing any information in such systems. Review of all public interfaces should be carried out at a specified frequency.

6.11.4 Sharing of IT Systems

airtel is recommended to share the IT systems within the group companies subject to the following requirements:

a. Compliance with the BISP/Africa;

b. Compliance of Confidentiality obligations under respective applicable agreements in relation to data accessible on the system(s);

c. Strictly protect Privacy rights of customers, and ensure customer data of any one company is not shared with any other group company or otherwise; and

d. The computer hardware, software and procedures should be highly secure from unauthorised access and misuse by employees of any other company or otherwise and restrict access of each company's data to the authorised employees of that particular company only.

6.11.5 Sharing of Intranet

a. The intranet site, where available, should be accessible to the permanent airtel Africa Employees only.

b. Further checks should be done from the HR, communications and any other relevant department the extent to which the material available on the intranet site is applicable to any other group company employees.

6.11.6 Controls over Data Mining Activities

Adequate controls shall be put in place to track and monitor all data mining activities.

6.12. Monitoring

6.12.1 Audit Logging

a. IT and Networks functions are required to ensure that the audit logs 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 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. It shall be ensured that the system administrators do not have permissions to erase or de-activate logs of their own activities.

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

6.12.2 Monitoring System Use

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

b. A log 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

   iv. Changes to, or attempts to change, system security settings and controls.

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 and a consolidated report

shall be prepared in a specified format for all reviewed monitoring activities. This report shall be presented to the Security SPOC from IT/ Networks functions.

6.12.3 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.

6.12.4 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.

6.12.5 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.

6.12.6 Clock Synchronisation

a. All computer clocks shall be set to agreed standards. 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 Network Time Protocol (NTP) servers deployed for each of the time zones in which airtel operates.

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 (BISP/Africa – 007)

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 airtel.

7.1.1 Responsibility

It is the responsibility of the IT and Networks 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 teleworking 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 Security SPOC 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.

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 airtel, 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 and Networks 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 Handbook.

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 airtel'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

g. A list of standard services that are not allowed in the internal network is formally documented and such services are disabled.

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 airtel IT network are provided to authorised users only and appropriate controls implemented to maintain the confidentiality, integrity and availability of information;

b. An updated list of all such connections is maintained;

c. Remote access to the network of airtel is allowed through secure channels only;

d. Remote access is allowed through pre-approved accounts only and monitoring is enabled for all such accounts;

e. Appropriate controls meeting the regulatory requirements are implemented, if remote access is provided to manufacturers or suppliers for diagnosis or maintenance activities;

f. Modems connected to the end user workstations/ laptops are configured to reject all incoming traffic initiated from external sources;

g. Where remote access through modem is required, it is recommended that modems are automatically disconnected after specified period of inactivity. These modems are to be activated only on need to have basis and deactivated immediately after use; and

h. Only approved remote control software are used in the network for remote connections.

7.5.2 Equipment Identification in Network

As an additional authentication control for remote access, the equipment identifier is recommended to be used to authenticate the equipment connecting to the critical information systems of airtel.

7.5.3 Segregation in Networks

The security of the airtel 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.

7.5.4 Network Connection Control

a. For shared networks, especially those extending across the boundaries of airtel, 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 restricted in airtel.

7.5.5 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.

7.5.6 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* and record the successful and failed system authentication attempts.

7.5.7 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 (*Refer section 7.5.1)*.

7.5.8 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 and/ or Networks functions shall be obtained and documented for the same.

c. For the information systems that contain critical business information, strong authentication and identity verification are required. Authentication methods alternative to passwords, such as cryptographic means, smart cards, tokens or biometric means are shall be used, where specified.

d. Appropriate authentication mechanisms shall be implemented for all systems.

7.5.9 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*.

7.5.10 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 and Networks 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.

7.5.11 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 10 minutes of inactivity, unless defined otherwise.

7.5.12 Limitation of Connection Time

IT and Networks function shall identify the applications and information systems that are catering to the sensitive information of airtel and/ or its customers and being accessed from external networks and Internet. These applications and information systems, as far as possible, shall have limitation on connection time-slot as an additional security control.

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 airtel. All applications shall be tested for information security requirements and be compliant to *Application Security Standard*. An application security assessment shall be conducted for the critical applications at regular intervals. Clearance from the airtel Africa Security Team shall be obtained prior to deploying application in the production environment.

7.6.1 Information Access Restriction

IT and Networks functions 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/ Networks functions 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 and Networks 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 airtel 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 airtel, to prevent any compromise and/ or destruction of business information.

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

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

e. Third party staff shall not connect their computing devices to the wired or wireless network of airtel, unless authorised by the Security SPOC of IT/ Networks function.

7.7.2 Teleworking

Teleworking requests shall be handled in accordance with the *Mobile Computing and Teleworking Procedure*. Adequate teleworking security measures shall be established and implemented. At a minimum the following shall be considered:-

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

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

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

8. Information Systems Acquisition, Development & Maintenance Policy (BISP/Africa – 008)

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 and Networks functions are responsible for the implementation and maintenance of the controls defined in this policy.

The IT and Networks 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 BISP/Africa and a sign off on the same shall be obtained from the airtel Africa Security Team 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.

c. Application security standard and checklist shall be developed and used for conducting the security assessment of the applications.

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. Vendor supplied software packages shall be maintained at the level that is supported by the vendor.

g. 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 strict 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/ bespoke 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 airtel and the third party.

b. The contract shall include that airtel reserves the right to audit quality and accuracy of software development and testing. Such software code shall have escrow arrangements.

8.6. Technical Vulnerability Management

8.6.1 Control of Technical Vulnerabilities

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

9. Information Security Incident Management Policy (BISP/Africa – 009)

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) having representation from all the business functions at the airtel Africa HO

It is the responsibility of the Executive Council at all the Circles to appoint representatives from each function to act as the OpCo Incident Response Team.

The Incident Response Teams at the airtel Africa HO and all the OpCos shall be responsible for the development and implementation of the controls defined in this policy.

It is the responsibility of all employees and third party staff to report any security incident that they observe or suspect to the IT Helpdesk. They shall also send an email to sirt@cc.airtel.com (where 'cc' is the country code of the respective OpCo) in 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 airtel.

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.

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. This shall be part of the Information Security Awareness Programme.

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.

9.6. Collection of Evidence

a. As per the legal requirements the evidences shall be collected during incident analysis, maintained and presented to the relevant authorities.

b. The evidence shall be collected in a manner that does not destroy its evidentiary value.

c. While collecting the evidence, the following shall be considered:-

   i. Applicability of evidence: the evidence can be used in a court of law; and

   ii. Weightage of evidence: the quality and completeness of the evidence.

10. Business Continuity Management Policy (BISP/Africa – 010)

10.1. Introduction

a. airtel understands the importance of continued availability of its key people, telecom products and services, infrastructure and processes supporting these products and services.

b. The Business Continuity Management Policy defines the intent of the airtel management to establish a Business Continuity Management System (BCMS) to counteract or minimise interruptions to key business activities. The interruptions could be due to natural or manmade disasters, or technology incidents which might convert into disasters.

c. Towards this intent, business continuity plans, site emergency management plans, call trees of functions at OpCos and airtel Africa HO sites and disaster recovery plans for Network Services Group (henceforth referred as NSG) and Information Technology (henceforth referred as IT) should be documented and tested.

d. The Business Continuity Management Policy defines the purpose, responsibilities, scope, framework, approach and objective to manage the business continuity management system within airtel. The organisation supporting Business Continuity Management System (henceforth referred as BCMS) shall have representation from all the business units along with NSG and IT which should ensure a structured development, implementation, exercising and review cycle of the BCMS.

e. This section of the BISP shall be communicated to all airtel employees and strategic partners. This section of the BISP shall be reviewed at least annually or whenever significant changes occur in the organization.

10.1.1 Purpose

a. The purpose of this policy is to establish the management's intent towards setting up and maintaining an effective BCMS. The process of establishing the BCMS should start with identifying business needs, carrying out current state assessment to determine business risks, developing recovery strategies and creating business continuity and disaster recovery plans (henceforth referred as BCP) for mitigating such business risks.

b. The BCP shall address the following requirements:-

   i. Continued adherence to contractual liabilities, statutory and regulatory requirements as decreed by the government or their representative bodies in the countries where airtel Africa operates.

   ii. Ensure customer satisfaction by delivering key products and services as per defined SLA's.

iii. Remove or minimise risks to customer acquisition, service availability, revenue continuity and people safety aspects at the time of disaster.

iv. Protect business critical infrastructure from identified threats.

v. Maintain market reputation of airtel and a competitive advantage at the time of disaster.

vi. Continued delivery of services from partners and vendors at the time of crisis.

10.1.2 Accountability and Responsibility

a. The Information Security Steering Committee (ISSC) shall be accountable for developing and maintaining the BCMS. The ISSC has delegated responsibility for implementing, testing and reviewing the BCMS to the Business Continuity Working Group (BCPWG) headed by the Global Chief Information Security Officer (CISO) with members from all functions at HO Airtel Africa and representatives from each OpCo. The CISO shall deploy dedicated business continuity resources to centrally manage the program.

b. At the OpCos the CEO/COO/MD shall be responsible for implementing, testing and reviewing the BCMS, while functional chiefs shall be responsible at airtel Africa HO.

c. The CEOs / COOs shall use their executive councils (henceforth referred as EC) and other existing resources within the OpCo to carry out business continuity tasks in addition to their own. Functional chiefs at airtel Africa HO shall, use existing resources within their functions to carry out business continuity tasks in addition to their own. Such resources shall have BCP specific KRAs as part of their annual goal sheets.

10.1.3 Scope of BCMS at airtel

a. This policy applies to all functions, their processes, sites, technology services and network elements, people, and strategic partners.

b. The BCMS at airtel has been developed to comply with requirements of BS 25999, which is a globally accepted standard for business continuity management.

c. The designated representatives of AIMB at airtel Africa HO and EC members at respective OpCos, as relevant, would define Recovery Time Objectives (RTOs) and Recovery Point Objective (RPOs) for all products and services offered by airtel.

d. The OpCos are supported by NSG and IT functions and shared services groups for delivery of product and service.

e. All business continuity plans spanning critical business processes, people safety, information technology, network elements and site safety should be documented, implemented and tested

across all OpCos and HO airtel Africa functions (customer services, supply chain management, finance, HR& Admin, sales and marketing, business excellence, president/CEO's office, legal and regulatory) and NSG & IT, towards achieving the recovery time objectives defined by the respective management boards.

f. Business continuity risks for third parties shall be mitigated through controls listed in the Bharti Third Party Security Policy (BTSP).

10.1.4 BCMS Approach for airtel

a. Business Continuity Management System for airtel is based on minimising impact to people; process, technology and site by ensuring continued availability of the SLRC model (Service Delivery, Legal & Regulatory compliance, Revenue Continuity and Customer Acquisition) for airtel.

b. SLRC model is a simplified version of the business model being used by airtel. The model encompasses the following aspects:

1. **S**ervice Delivery – This indicates activities undertaken for the delivery of products and services through NSG and IT. The BCMS aims for continuity of delivery of such products and services to the customer, in the event of a disaster.

2. Legal & Regulatory Compliance - This indicates the activities undertaken to ensure compliance with the legal and regulatory requirements. The BCMS aims for continuity of compliance activities in the event of disaster.

3. **R**evenue Continuity– This includes processes undertaken for collection of revenue from existing customers for services utilized and from new customers for services provisioned. The BCMS aims for continuity of revenue streams in the event of disaster.

4. **C**ustomer Acquisition – *This r*efers to the processes undertaken to acquire new customers for provision of services. The BCMS aims for continuity of delivery of processes pertaining to acquisition of new customers in the event of disaster. These processes are primarily executed at OpCos.

c. The management has laid down the following priorities for the SLRC streams:

Priority 1: Service Delivery

Priority 2: Legal & Regulatory Compliance

Priority 3: Revenue Continuity

Priority 4: Customer Acquisition

d. BCMS for airtel should ensure safety of employees and sites, service availability to customers and continuity of key business processes in case of a disaster.

e. Business processes would be classified as "Critical", "Essential" and "Non- Essential" based on their criticality ratings. Criticality of business processes shall be based on Maximum time to resume (MTR) values. Maximum time to resume is the duration after which airtel's viability to conduct business is irrevocably threatened if product and service delivery cannot be resumed. A Time to Normalcy (TTN) value will also be identified basis which the time period within which the process would resume under Normal scenario.

f. Processes with MTR less than/equal to 72 Hrs would be termed as "Critical", processes with MTR greater than 72 Hrs but less than/equal to 2 weeks would be termed as "Essential" and processes with MTR greater than 2 weeks would be termed as "Non-Essential". Business continuity plans shall be written for all critical and essential processes. No recovery would be planned for "Non-Essential" processes.

g. IT and Network Technology: Impact to IT and network infrastructure, shall be mitigated through resiliency at design stage , on-going architectural reviews, identification of single points of failures through FMEA, identification of mitigating controls and their costs and implementation of business approved controls so as to minimise/mitigate such single points of failure.

   i. Impact to IT application, shall be mitigated through identifying business critical applications, identifying their MTR and RPO, sign off from the business on these MTR and RPO values and implementation of DR solution so as to meet business needs.

   ii. The DR solution along with DR processes should be implemented in such a way, so as to provide the product/service/application to the business within signed off MTR and RPO, which includes the time for invocation of disaster.

   iii. Disaster recovery plans shall be written for IT and NSG verticals and shall ensure continuity of IT and network operations.

   iv. There shall be specific immediate disaster response teams and a well-defined methodology for invocation of business continuity and disaster recovery plans which shall be documented in the Crisis Management Procedure.

h. Site: Site risk assessments shall be carried out at regular intervals and relevant controls shall be put in place by respective site owners to minimise risks of site disruption.

i. People: Impact to people shall be mitigated through awareness sessions and appropriate communication mechanisms e.g. call trees at the time of crisis. All Employee call trees shall be

implemented at all OpCos, to ensure airtel has an effective means to communicate and determine safety of its employees in case of a crisis situation.

j. Third Party Vendors: Business continuity risks for third parties shall be mitigated through controls listed in the Bharti Third Party Security Policy (BTSP). Function heads within airtel who liaise with such third parties would be responsible to ensure implementation of such controls by the concerned third parties.

10.1.5 Acceptable Level of Risk

a. Acceptable level of risk shall be defined based on decisions taken by the ISSC, and OpCos where the services/ products are restricted to only that OpCo.

b. Acceptable level of risk for NSG and IT shall be recommended by Network functional chief and IT functional chief and finally approved by the ISSC. Similarly, acceptable level of risk at the OpCo shall be recommended by Executive Council (EC) and approved by OpCo CEO/COO.

c. IT would implement DR solutions so as to achieve MTR and RPO signed off by the business. This would be basis a Risk Signoff and acceptance document signed off by the business functions

d. MTR would be defined for all products and services offered by airtel. The decisions on MTR for products and services offered by airtel Africa shall be taken by respective management boards and shall be signed off by respective functional chiefs, and OpCo CEO/COO/MD, where necessary.

e. NSG would identify MTR for partial (should be a quantifiable figure) and 100% recovery of services offered from each network location. These site wise values would be computed and finalized by NSG, and signed off by respective functional chief and ISSC. NSG would aim to put in place mitigating controls till such time the network architecture is able to recover each product and service within MTRs signed off by respective management boards.

f. The products and services MTRs signify the risk appetite of the airtel management. The MTRs signed off by various functional chiefs are as follows:

Mobile Services	
Mobility Products	**MTR**
Voice Services	
Post-paid Voice	1 Hour
Prepaid Voice	1 Hour
Value Added Services	
SMS (P2P, P2A, A2P)	2 Hours
GPRS	2 Hours
Blackberry Services	2 Hours
Caller Ring Back Tone/Hello Tunes	2 Hours
Missed Call Alerts	2 Hours
Subscription Services	2 Hours
Toll Free Numbers	2 Hours
M-Commerce	2 Hours
airtel Live	2 Hours
On Demand Services	2 Hours
airtel Mate	2 Hours

Enterprise Services (as per product offering)	
Enterprise Services Products	**MTR (suggested for new launches)**
Domestic Voice	
NLD Voice - Category C	4 Hours
NLD Voice - Category A	40 Minutes
ISDN – PRI	3 Hours
ISDN-BRI	5 Hours
Toll Free Number	2 Hours
Voice Line	4 Hours
Post-paid Voice	1 Hour
Prepaid Voice	1 Hour
SMS	2 Hours
VAS (Mobility)	2 Hours

Blackberry	2 Hours
airtel Mate	4 Hours
Domestic Data	
MPLS	4 Hours
Internet	4 Hours
NLD Leased Lines	3 Hours
VSAT	2 Hours
Managed Data Services	NA
International Voice	
Wholesale Voice Termination (ILD Voice)	2 Hours
Global Hubbing	2 Hours
ITFS	2 Hours
airtel Call Home (ICS)	1 Hour
Wholesale Calling Card	1 Hour
International Data	
IPLC	2 Hours
Conference Services	
Bridge	30 Minutes
Link	3 Hours

10.1.6 Level of Recovery

a. There shall be a defined level of recovery for all critical business processes, products and services and IT applications at a point in time (MTR /RTO). The level defines the percentage of resources that would be recovered at RTO after occurrence of a disaster. Recovery Time Objective (RTO) is the target time set for resumption of product and service delivery after an incident; or resumption of performance of an activity after an incident; or recovery of an IT system or application after an incident. The level of recovery should start with a pre agreed percentage of resources starting from the RTO and should be ramped up to 100% over a period of time. (The recovery time objective shall be less than the maximum tolerable period of disruption)

b. The level of recovery for business processes, products and services and IT applications at the MTR and the time required to ramp to 100% operations shall be defined by the functional chiefs and OpCo for their respective functions.

c. **Processes:** The level of recovery defined for critical processes shall be in three levels, first recovery at RTO, second recovery level at interim MTR value and then complete recovery at 100% level, point of normalcy.

d. **Products and Services:** The level of recovery defined for products and services shall be in two level, first recovery at partial level and then complete recovery at 100% level.

e. **IT Applications:** The level of recovery defined for critical IT applications shall be in two level, first recovery at partial level and then complete recovery at 100% level. Here, partial level would mean availability of application from alternate location while 100% level is application availability back from primary location.

10.2. Policy Statement and Objective

Business Continuity Management System for airtel shall be focused on maintaining continued delivery of products and services to customers, honouring contractual and regulatory obligations by minimising impact to service availability, revenue continuity and customer acquisition.

This shall be ensured by the following:-

a. Delivery of an acceptable level of products and services to the customer during a disaster.

b. Statutory, legal and regulatory requirements of the business shall be met;

c. Shareholder Value and market reputation shall not be affected.

d. SLRC model shall be executed in the agreed order of priority during a disaster.

10.3. BCMS Framework

airtel's BCMS is based on the Plan-Do-Check-Act (PDCA) model:

a. **Plan:** airtel shall establish a BCMS policy expressing the management's intent towards BCP along with a defined BCMS governance structure. Planning involves studying the as-is scenario, identifying options of mitigating controls and approvals and budgeting of best possible controls to minimise risks of disruption;

b. **Do:** This stage involves documenting plans, implementing mitigating controls and training of resources;

c. **Check:** This stage involves testing of plans, conduct third party assessments to identify compliance on BCP requirements per BTSP, monitoring and review of BCMS;

d. **Act:** Carry out on-going change management, internal audits and management reviews of the BCMS. Build improvements into plans, based on test & review results improve documented plans.

The following are the key stages in the process of developing and maintaining BCMS for airtel:-

10.3.1 BCMS Governance

a. The ISSC shall have the authority to build, maintain and operate the BCMS at a pan airtel level. The ISSC shall be accountable for oversight, initiation, planning, maintaining, approval, exercising and audit of the BCP across all units through the established BCMS;

b. The ISSC shall delegate responsibility to relevant resources within all functions at a pan airtel level to build, maintain and operate the BCMS.

c. The business unit head (CEO/ COO/ MD) shall own the development, implementation, maintenance and testing of Business Continuity Management System (BCMS) at the OpCo.

d. BCMS Governance structure shall contain people responsible, accountable, consulted and informed for various activities within the BCMS. It shall also define the roles and responsibilities for ISSC, BCPWG, Global CISO, CBC, CEO/COO/MD, Unit BCP Coordinator, Unit BC Process Champions, Unit's top management, Immediate Disaster Response (IDR) Teams and all such resources who would be held responsible to build, maintain and operate the BCMS;

e. Well defined BCMS Governance model shall establish the business continuity framework to achieve the objectives defined in this policy.

f. The defined BCMS governance structure shall be reviewed every year by airtel. The BCMS Governance methodology shall be detailed out in BCMS Governance Procedure.

10.3.2 BCMS Business Impact Analysis

a. airtel shall carry out Business Impact analysis (henceforth referred as BIA) for all:

   i. Products,

   ii. Business processes and

   iii. Applications supporting critical business processes.

b. airtel shall define and document an appropriate methodology for BIA that shall enable the organization to identify business critical processes, resources and applications needed to support its key products and services along with respective maximum time to resume (MTR) and recovery time objective (RTO) values. The BIA results shall be revisited on an annual basis.

   i. MTR for business wise products shall be defined by respective functions and signed off by respective functional chiefs.

   ii. MTR and RTO values for business processes shall be defined by functional process champions and shall be approved by the respective functional head. The CEO/COO/MD shall finally sign off MTR and RTOs for all business processes of that OpCo.

iii. RTOs and RPOs of IT applications supporting business processes shall be defined by the respective process heads at OpCos and signed off by the respective CEO/COO/MD.

c. The BIA methodology would define methodology to identify, minimum operating requirements (henceforth referred as MOR) to recover the identified critical processes, categorize its activities according to their priority for recovery and identify all dependencies relevant to the critical activities.

d. Business Impact Analysis for products, applications and process layer shall be reviewed on a bi-annual basis. The BIA methodology shall be detailed out in the BCMS Business Impact Analysis Procedure.

10.3.3 BCMS Risk Assessment

a. airtel shall carry out risk assessment (henceforth referred as RA) for all critical business processes, support resources and sites at pre-defined frequencies. RA shall also be carried out for IT and network infrastructure to identify points of failure.

b. airtel shall define and document an appropriate method for RA that shall enable the organization to understand the threats to and vulnerabilities of its critical business processes, supporting resources including those provided by any third party providing services to airtel, sites and its IT and network infrastructure. Risk assessment for the technology layer shall be based on failure modes as the recovery strategy and the response will directly depend on the kind of technological failure. RA shall be reviewed on an annual basis; in addition control implementation as well as secondary risk arising out of control implementation shall also be reviewed on an annual basis.

c. Through the RA process, the ISSC shall understand the risk that would arise if an identified threat exploits the vulnerability and becomes an incident causing business disruption; and the risks arising out of the RA exercise shall be treated, terminated, transferred or accepted by the respective risk owner.

d. The ISSC shall monitor the implementation of controls by the risk owners against risks arising out of the RA exercise.

e. The RA methodology shall be detailed out in the BCMS Risk Assessment Procedure.

10.3.4 BCMS Recovery Strategies

a. Process: airtel shall develop recovery strategies for critical business processes to minimise the period of disruption and limit the impacts that such disruptions may have on delivery of key products and services, mitigate risks on account of people safety issues, site safety, business

process disruption, technology and network disruptions. All recovery strategies shall be reviewed on a bi-annual basis.

b. Recovery strategies for critical business processes shall ensure recovery within signed off process RTOs and MTRs.

c. Products and Services: The recovery strategies would be aligned for effective delivery of key products and services and risk acceptance for residual risks would be signed off by respective management boards. airtel has planned to have an impact based planning for critical enablers during crisis situation and hence recovery strategies shall be aligned to mitigate the impact of the incident.

d. People: People safety issues would be addressed by adequate training (safety issues, evacuation plans etc.) and by establishing effective all employee communication methodologies to ensure their safety during a disaster.

e. Site: Recovery strategies for safety for sites should identify and implement controls to mitigate risks emanating out of the risk assessment exercise.

f. Technology: Recovery Strategies for IT and network infrastructure should ensure that points of failure within the infrastructure are mitigated and disruption risks are either eliminated or reduced to the bare minimum.

g. The Recovery Strategy methodology shall be detailed out in the BCMS Recovery Strategy Procedure.

10.3.5 BCMS Plan Documentation and Implementation

a. airtel shall document business continuity plans (henceforth referred as BC Plans) for all OpCos. The CEO / COO / MD at OpCos and functional chiefs at airtel Africa HO, IT and NSG shall own and maintain these plans. The BC Plans shall cater to employee safety, L&R compliance, crisis management, crisis communication, business process recovery, IT and network recovery, site emergency management, plan activation and deactivation steps.

b. IT and NSG shall document disaster recovery plans (henceforth referred as DR Plans). The DR plans shall be owned and maintained by the respective IT and NSG vertical heads and signed off by Director IT and Director NSG. The DR plan shall contain network diagram, details of critical network nodes, connectivity diagram, data capturing details of transmission network, recovery steps and incident escalation matrix, etc. for NSG and shall contain application interface diagram, details of critical applications, connectivity diagram, details of transmission, LAN-WAN IT network, application recovery work instructions (both primary to alternate and alternate to primary) and incident escalation matrix, etc.

c. The disaster recovery plan shall include business continuity requirements.

d. The BC Plans and DR plans shall have primary and secondary members identified for critical BCMS roles at the units, IT and NSG.

e. airtel shall follow a defined update and maintenance framework for the BCMS, which shall be detailed in the BCMS procedure documents. Plan owners shall be responsible to ensure that there is a defined process to monitor changes in the operating environment and that the BCMS is kept updated so as to align to these changes. In addition, the plan owners shall update and maintain the documents and carry out review of the entire BCMS at periodic intervals.

f. airtel shall carry out on ground implementation of all BC Plans and DR Plans. It would be the responsibility of plan owners to ensure that documented business continuity strategies are implemented as defined in the plans. Plan owners shall ensure implementation of the plans as and when the plans are reviewed and revised.

g. The BCMS plan documentation and implementation details shall be detailed out in the BCMS Plan Documentation and Implementation procedure.

10.3.6 BCMS Emergency Response

a. airtel shall have well defined emergency response framework and a systematic methodology of dealing with and avoiding risks/threats to business, identified as part of the risk assessment exercise.

b. Emergency response processes shall involve preparing for disaster by putting in place mitigation controls as part of Pre Crisis Preparation, disaster response (e.g. emergency evacuation, quarantine, mass decontamination, etc.), as well as supporting, and recovery after a disaster;.

c. airtel shall identify top 15 threats which shall emanate from the risk assessment exercise. These threats shall be reviewed on an annual basis. The emergency response shall be planned to address these top 15 threats.

d. The steps for readiness, emergency response and recovery actions to be taken corresponding to top 15 threats shall be documented in BCMS Emergency Response Procedure.

10.3.7 BCMS Crisis Management

a. CEOs / COOs / MDs at OpCos and functional chiefs at airtel Africa HO shall ensure that all sites within their jurisdiction shall have well defined incident management processes to cater to employee safety, IT / network outages, site safety etc. The incident management processes shall cater to all scenarios arising out of identified top 15 threats, of that unit, which may result in disruption of operations.

b. airtel shall implement a comprehensive crisis management program. There shall be Immediate Disaster Response teams (henceforth referred as IDR teams) at OpCos, IT, NSG and a central IDR team for airtel Africa HO. The crisis management program shall follow a decentralised

model where disasters with local impact shall be handled by local IDR teams and escalations if any shall be referred to the central IDR teams.

c. The crisis management plan shall be triggered based on escalations from individual incident management programs. Functional Incident management plans should document appropriate triggers for invoking crisis management plans.

d. The crisis management plan shall define guidelines for assessing escalations from incident management programs before declaring such events as a BCP event.

e. There shall be defined guidelines within the crisis management plan to assess the impact of an incident.

f. The crisis management team shall declare "crisis" based on guidelines defined in Crisis Management Procedure, which shall document a well-defined process for crisis declaration for OpCos/airtel Africa HO, IT and NSG. The site emergency management plan, business continuity and disaster recovery plans shall be activated basis the crisis declaration by CMT.

g. There shall be a defined crisis communication model for communicating with Internal and external stakeholders during crisis. Internal stakeholders shall include employees and family members of employees (for certain incidents), senior management (e.g. AIMB) and third party employees. External stakeholders shall include media and press, regulatory and government agencies, customers, third party service providers, strategic partners, suppliers etc.

h. The Crisis management program shall be detailed out in the BCMS Crisis Management Procedure.

10.3.8 BCMS Training and Awareness

a. airtel shall have a defined BCMS training and awareness program at OpCos and airtel Africa HO.

b. CEOs /COOs /MDs/functional chiefs shall ensure that personnel who are assigned business continuity roles and responsibilities shall participate in the BCM training program to ensure building the competency required as per the defined roles and responsibilities.

c. A training needs analysis shall be carried out for BCMS roles required during development, implementation and maintenance of BCMS at the business unit and for roles during crisis. Training need analysis shall be performed for unit BCP coordinator, functional planners, process champions and senior management for roles during development, implementation and maintenance of BCMS; and IDR team members (CMT, DAT, RST and ORT), fire wardens, incident response personnel/ facility manager for roles during crisis. Based on the results of the need analysis, a comprehensive training program shall be drafted with a clear roadmap to get such personnel adequately capable of operating the BCMS;

d. The training program should have clearly measurable Key Performance Indicators (henceforth referred as KPIs) to ensure that the program attains the desired effectiveness and that the necessary competence has been achieved;

e. As part of the BCMS training program, records of education, training, skills, experience and qualifications of the trainees shall be maintained by HR.

f. The methodology for BCM training shall be detailed out in the BCMS Training and Awareness Procedure.

10.3.9 BCMS Exercising

a. CEOs / COOs / MDs / functional chiefs shall ensure that all plans documented as part of the BCMS are tested and exercised on an on-going basis to ensure that the plans are fit for purpose and effective.

b. IT and NSG verticals heads shall conduct DR tests at least on a bi-annual basis.

c. All Employee Call trees (SMS mode or Manual mode or both) shall be tested at least on a bi-annual basis.

d. Process recovery testing for critical business processes shall be conducted at least on an annual basis encompassing all of the people, site and technology enabler failure scenarios.

e. Functional planners shall conduct walkthrough of BC plans as part of self-assessment exercise least on an annual basis;

f. Exercising methodologies shall be clearly defined, where such exercises should be scoped, signed off by the respective functional heads (CEOs / COOs /MDs/functional chiefs), monitored for adherence to plan and reporting of results of the exercises to the ISSC. The ISSC shall review the test results at regular frequencies. A comprehensive test program shall be developed and promulgated across all units; this program shall be reviewed on an annual basis.

g. The results of the tests shall be used for continual improvement of business continuity plans.

h. The methodology for BCMS Exercise and testing shall be detailed out in the BCMS Exercising Procedure.

10.3.10 BCMS Control of Documents and Records

a. There shall be a defined methodology to have control of all BCMS documents. Records and guidelines shall be defined to ensure the identification, storage, security and safety of BCMS documents and records. It should be ensured that critical BCMS documents and records remain legible, and are readily identifiable and retrievable.

b. Controls shall be established over BCMS documentation to ensure that documents are approved for adequacy prior to issue; documents are reviewed and updated as necessary and the current revision of documents are identified in the master list of documents; documents are made available at points of use; and distribution of documents is defined and controlled.

c. The methodology for control of BCMS documents and records shall be detailed out in the BCMS Control of Documents and Records Procedure.

10.3.11 BCMS Vital Records Management

a. All units shall identify and classify vital records required for business continuity purpose.

b. Relevant strategies should be implemented for vital records, so that they are made available for use in case of disaster leading to business disruption. The strategies should have a process for creation, classification, storage, retrieval and disposal of vital records with clear responsibilities assigned for each activity so as to make the vital records available during a disaster.

c. The methodology for vital record maintenance shall be detailed out in the BCMS Vital Record Management Procedure.

10.3.12 BCMS Pandemic Response

a. As part of the BCMS, airtel shall implement and maintain pandemic response framework to ensure employee health & safety and to prevent or contain potential business disruptions and resume business operations within MTR during any pandemic situation;

b. Based on severity of impact of pandemic on airtel, a multi staged pandemic impact matrix shall be defined. airtel shall map a response strategy for each stage.

c. The Pandemic Task Force (henceforth referred as PTF) at airtel Africa HO shall be the responsible for taking decisions on the pandemic response decisions for airtel. The PTF would be supported by OpCo Pandemic Task Forces (OPTF) at the OpCo

d. The PTF shall be responsible to monitor implementation of controls at airtel Africa HO and at a Pan airtel level. The OPTF shall implement controls at the OpCos based on decisions taken by the PTF.

e. The methodology for Pandemic response shall be detailed out in the BCMS Pandemic Response Procedure

10.3.13 BCMS Call Tree Development, Maintenance and Testing

a. airtel shall have a defined methodology for communicating with all employees within an OpCo during a crisis. The methodology shall involve manual (calling) mode and SMS based communication;

b. The methodology should ensure that the units have a process in place to keep the call trees updated and tested at regular frequencies so that the same can be effectively used when required.

c. The functional planners shall ensure update of functional call trees as per the defined frequency.

d. There shall be a defined frequency to test the call trees to ensure the effectiveness of the methodology.

e. The methodology for all employee call tree shall be detailed out in the BCMS Call Tree Procedure.

10.3.14 BCMS Monitoring

a. airtel shall have a methodology for maintaining and monitoring the BCM arrangements at the business units;

b. CEOs/ COOs/ MDs /functional chiefs through their nominee BCP coordinators shall carry out monitoring of the BCMS to ensure that the update and maintenance of the BCMS is being carried out effectively by the OpCos and Airtel Africa HO.

c. There shall be a Management Review by OpCo heads and their executive councils for the BCMS at the business OpCo function as per pre-defined frequency.

d. There shall be a defined self-assessment program for ensuring that the business continuity plans are up to date and modified as required.

e. Third party audits shall be planned as part of the BCMS program and the business unit head shall be accountable; the responsibility of facilitating the third party audits shall remain with the nominated BCP coordinator.

f. The methodology for self-assessment, management review and third party audit of the BCMS shall be detailed in the BCMS Monitoring Procedure.

10.3.15 BCMS Internal Audit

a. There shall be a defined BCMS internal audit program for the BCMS of every business unit at both the OpCos and airtel Africa HO.

b. Internal audit shall be conducted for BCM activities defined at the business unit, business functions and facilities/sites.

c. Independent internal BCMS audits shall be planned and conducted periodically to validate the effectiveness of the BCMS.

d. These audits shall be conducted by personnel who are nominated as auditors by unit heads. In order to maintain independence the auditors should be from the function other than the function to be audited. Results of such audits shall be presented to the unit head and the ISSC at OpCos and airtel Africa HO respectively.

e. Internal audit shall be planned at least once a year.

f. The methodology for BCMS internal audit shall be defined in BCMS Internal Audit procedure.

10.3.16 BCMS Corrective Actions and Preventive Actions

a. airtel shall ensure continual improvement of BCMS through the application of corrective and preventive actions.

b. The triggers for corrective and preventive actions can be from BCMS testing, changes in the organization, incidents and audit observations from internal and third party audits.

c. A methodology shall be established to ensure that any corrective and preventive action taken shall be appropriate to the magnitude of the problems and commensurate with the business continuity policy and objectives. Also, changes arising from corrective and preventive actions shall be reflected in the BCMS documentation.

d. The corrective and preventive actions taken shall be reviewed in self-assessments, internal audits and management reviews.

e. The methodology for corrective and preventive actions shall be detailed out in the BCMS Preventive and Corrective Action Procedure.

10.4. Limitations and Exclusions

a. A national disaster e.g. country wide political instability, terror attacks with wide ranging national impact, nation wide pandemic spread, etc. shall be excluded from the scope of BCMS; however, all Crisis Management Plans will remain within the scope, especially aspects dealing with people safety;

b. Any product(s), service(s) and process(s) that have an RTO over 2 weeks is termed an non-critical and shall be excluded from the scope of BCMS;

c. Processes followed by strategic partners and Third Party Vendors to support airtel's operations shall not be a part of the documented BC Plans/DR Plans for airtel. Partner's business

continuity risks shall be managed through contractual obligations and third party risk assessment process.

10.5. Glossary

BCP	Business Continuity and Disaster Recovery Plan
BCMS	Business Continuity Management System
OpCo	Operating Company
BISP	Bharti Information Security Policy
BTSP	Bharti Third Party Security Policy
BS	British Standard
ISSC	Information Security Steering Council
BCWG	Business Continuity Working Group
CISO	Chief Information Security Office
PDCA	Plan Do Check Act
SLA	Service Level Agreements
RTO	Recovery Time Objectives
RPO	Recovery Point Objectives
SMS	Short Message Service
PTF	Pandemic Task Force at airtel Africa HO
OPTF	OpCo Pandemic Task Force at Units
EC	Executive Council
IT	Information Technology
CEO/COO	Chief Executive Officer/Chief Operating Officer
BS 25999	British Standard 25999
BC plans	Business Continuity Plans
DR Plans	Disaster Recovery Plans
IDR teams	Immediate Disaster Response teams
RA	Risk Assessment
KPI	Key Performance Indicator
PACA	Preventive Action-Corrective Action
NSG	Network Services Group

11. Compliance Policy (BISP/Africa – 011)

11.1. Introduction

The *Compliance Policy* provides direction to design and implement appropriate controls to meet legal, regulatory and contractual requirements within the business functions of airtel.

11.1.1 Responsibility

It is the responsibility of the Legal and Regulatory function to identify the relevant legislation and regulations for business operations and intellectual property rights.

It is the responsibility of the HOD of each function to ensure that his/ her function meet the requirement of the BISP/Africa and relevant legal and regulatory controls.

It is the responsibility of the Administration, IT and Networks functions to implement appropriate controls ensuring prevention of misuse of business information and facility. The IT and Networks functions are also responsible for identifying and maintaining relevant cryptographic controls as per legal, regulatory and contractual requirements. They may seek support from the Legal and Regulatory function for the identification of such requirements.

It is the responsibility of all employees to protect the records and information assets of airtel and adhere to the Information Privacy Policy (IPP).

11.2. Policy Statement and Objective

Compliance with legal, statutory, regulatory, contractual obligation and/ or security requirements is of extreme importance. All business functions shall be committed to adhere to these requirements and aim to embed a compliance culture in the organisation.

The objectives of this policy are to:-

a. Address Corporate Governance on behalf of the share-holders;

b. Address the privacy of customer information held by airtel;

c. Promote a positive ethical and compliance culture within airtel;

d. Avoid breaches of any legal, statutory, regulatory and/ or contractual obligations as well as security requirements; and

e. Ensure that employees and third party staff understand and adhere to the legal, statutory, regulatory, and contractual and security requirements which may have an impact on their daily activities.

11.3. Compliance with Legal Requirements

11.3.1 Identification of Applicable Legislation

A list of all relevant statutory, regulatory and contractual information security requirements shall be maintained by the Legal and Regulatory function. Information security aspects specified in any circular or note released by legal and/ or regulatory authority shall be complied with.

11.3.2 Intellectual Property Rights (IPR)

'Intellectual Property' is the original expression that derives its intrinsic value from a creative idea and shall be considered as a critical asset. The ISSC shall provide its endorsement to the information identified as intellectual property. The classification of intellectual property shall be done as per the *Information Classification Standards*. Intellectual Property Rights shall be included in all contracts. IPR Handling shall be done as per the *Information Labelling and Handling Procedure*.

11.3.3 Protection of Organisational Records

a. The HODs of functions shall ensure the retention of organisational records of their business functions in accordance with legislative, regulatory and contractual requirements.

b. The mechanism used for storage and handling of organisational records shall ensure clear identification of records and the period for which records need to be maintained as defined by the legislation or regulations.

c. The organisational records shall be maintained and stored as per the Control of Records Procedure.

d. The relevant business, legal and regulatory requirements shall be identified and documented for storing the information marked as 'Confidential' or 'Strictly Confidential'. These documentations shall also specify the period for which such information needs to be stored.

e. The maintenance period of 'Confidential' and 'Strictly Confidential' information shall be limited as per the business, legal and/or regulatory requirements.

f. Data that is no longer required for business, legal and/ or regulatory purpose shall be securely disposed of as per the *Media Disposal Procedure*.

g. 'Strictly Confidential' and 'Confidential' information shall be reviewed at regular intervals to ensure its retention as per the business, legal and/ or regulatory requirements.

h. *Information Labelling and Handling Procedure* and *Media Disposal Procedure* shall be applicable to all organisational records.

i. Backup of organisational records shall be done as per the *Backup Policy (Refer section 6.7)*.

j. Access control to organisational records shall be implemented in accordance with the *Access Control Policy (Refer BISP/Africa-007)*.

11.3.4 Data Protection and Privacy of Personal Information

a. The data protection and privacy of personally identifiable information at airtel shall be ensured in accordance with the Information Privacy Policy (IPP).

b. Strong implementation of privacy safeguards and consistent enforcement of information security controls shall be ensured to address privacy and personal data protection.

c. A Privacy Breach and Media Response Plan shall be developed. This plan would contain the steps to be taken in case of a privacy breach and for handling of the media response.

d. Privacy Compliance Systems, both network based and host based, shall be implemented.

e. Security technologies shall be implemented to enforce encryption and database extrusion detection.

f. Appropriate technical and administrative controls shall be identified and implemented to protect personal information pertaining to users and customers.

g. Responsibility for handling personal information and ensuring the awareness of the data protection principles shall be dealt with as per relevant legislation and regulations.

h. Personal records shall be maintained and stored as per the *Control of Records Procedure*.

i. Management and hierarchy ownership of personal records shall be defined.

11.3.5 Prevention of Misuse of Information Processing Facilities

a. Controls shall be implemented to prevent employees and Third Party staff from accessing the information, information systems and/ or facilities for unauthorised purposes.

b. Legal advice shall be sought in writing prior to monitoring the personal information of the user/ customer and record of the same shall be maintained.

11.3.6 Regulation of Cryptographic Controls

a. It is recommended that cryptographic controls are identified as per the relevant agreements, laws and regulations.

b. Legal advice shall be sought to ensure compliance with all laws and regulations. Suitable procedure for compliance assurance shall be documented and maintained by the IT and Networks functions with support from the Legal and Regulatory functions.

c. Sensitive data should be rendered unreadable at all the locations of its storage. These locations include, but are not restricted to, databases, portable digital media, backup logs, audit logs, etc.

11.3.7 User Licence Management

IT/Networks functions shall identify and comply with the licensing requirements for information assets including proprietary software, application systems, which typically limit the use of application to specified machines or creation of the backup copies. Following controls shall be enforced:

a. Awareness sessions to the employees and third party staff for using only legal copies of software;

b. Maintenance of Asset register of licenses for the software/hardware products;

c. Monitoring of the use of licenses;

d. Implementation of controls to ensure the use as per license agreement(s); and

e. Conduct of regular checks to ensure that only authorised software and licensed products are installed on the servers, laptops, workstations, networks devices, etc.

11.4. Compliance with BISP/Africa and Technical Compliance

11.4.1 Compliance with BISP/Africa

The HOD of each function shall ensure that BISP/Africa and related procedures are implemented in his/her function to meet the desired compliance.

11.4.2 Technical Compliance Checking

a. IT and Networks functions are required to conduct technical compliance checking at regular intervals either manually or with the assistance of automated tools, which generate a technical report for subsequent interpretation by a technical specialist. The automated tools employed for this purpose shall be approved by the Global CISO.

b. All functions are required to obtain a security clearance for all new projects, products, applications, services, etc. from the airtel Africa Security Team during their initiation and prior to deployment in production environment.

c. Technical compliance checking shall cover penetration testing and vulnerability assessments, which could be carried out internally or by independent experts specifically contracted for this purpose.

d. Technical compliance checking shall be carried out as per the *Vulnerability Management Procedure*.

e. All identified vulnerabilities shall be closed as per the *Vulnerability Management Procedure*.

f. The *Information Systems Acquisition, Development and Maintenance Policy (Refer BISP/Africa – 008)* shall be adhered to, for the vulnerability assessment and penetration testing of the software applications and the information systems where software applications are installed.

11.5. Information Systems Audit Considerations

11.5.1 Information Systems Audit Controls

a. Audit requirements on the operational systems shall be planned, documented and agreed in order to minimise the risk of disruptions to business processes.

b. Copies of the system files shall be provided for appropriate protection till it is required.

11.5.2 Protection of Information Systems Audit Tools

a. All information audit systems/ tools shall be protected to prevent their misuse.

b. The authorisation process for acquiring, testing and maintaining the audit tools shall be followed.

12. Cryptography Policy (BISP/Africa – 012)

12.1. Introduction

The *Cryptography Policy* defines the security standards and requirements associated with the use of cryptographic services within airtel. It is intended to define the required protection level to maintain the confidentiality, integrity and authenticity of the confidential information assets and sensitive application systems of airtel. The specific details of the cryptographic controls are mentioned in the *Cryptography Standards*.

12.1.1 Responsibility

The IT and Networks functions are responsible for the identification of the information assets and services that require encryption controls. They are responsible for the implementation and maintenance of the appropriate cryptographic controls as per the *Cryptographic Policy*. They may seek the support from the Legal and Regulatory function for the identification of the applicable cryptographic controls that need to be implemented as per the legal or regulatory requirements.

All employees are required to read, understand and follow the responsibility specified in the cryptography section of Information Security Handbook.

12.2. Policy Statement and Objective

Confidentiality, integrity, authenticity and non-repudiation of business critical information during its transmission over un-trusted networks shall be maintained and legal and regulatory requirements of cryptographic controls shall be complied with.

The objectives of this policy are to establish and implement the controls to maintain the following attributes of information:-

a. Confidentiality i.e. denying unauthorised access to information;

b. Authenticity i.e. validating the source of the message, to ensure that the sender is properly identified;

c. Integrity i.e. providing the assurance that the message is not modified, accidentally or intentionally; and

d. Non-repudiation i.e. establishing that a particular sender has sent the message so that they cannot deny having sent the message at a later date.

12.3. Product Approval and Baselining

a. All encryption products and processes deployed on information assets shall be approved by the Global CISO before deployment. These products shall be configured to satisfy the minimum

baseline standards established and maintained to support the BISP/Africa requirements. The Head of IT Security/ Head of Networks Security shall ensure the conduct of a risk assessment and shall maintain a list of approved encryption algorithms and the acceptable key lengths for each algorithm. This list shall be made available to all system and network administrators.

b. The procedures shall be developed for the following:-

   i. The algorithms that are to be used to encrypt the information as per the *Information Classification Standard* and *Asset Management Policy* (Refer to BISP/Africa – 003). The algorithms shall take into consideration symmetric and asymmetric encryption;

   ii. The key lengths that could be used for both symmetric and asymmetric algorithms; and

   iii. Modes of operation of the recommended algorithms.

12.4. Encryption Techniques

a. airtel shall support the encryption algorithms suitable for its business needs. Use of a particular encryption algorithm to ensure privacy and integrity of information shall be decided by the IT/ Network functions in consultation with Global CISO based on the following:-

   i. Risk assessment;

   ii. Customer requirement(s); and

   iii. Regulation/ Law/Standards and compliance requirement(s).

12.5. Public Key Infrastructure

airtel may choose to setup its own internal certifying authority or avail the services of an external provider.

12.5.1 PKI - airtel as Internal Certifying Authority

a. airtel as Internal Certifying Authority (CA) shall provide the following services:-

   i. Issuing the digital certificates;

   ii. Key management; and

   iii. Key recovery.

b. The internal CA system shall be installed and managed securely with the appropriate physical and logical controls.

c. airtel as the internal CA shall keep a secure backup of its private keys. The backed-up keys shall be stored in encrypted format and protected from environmental and physical threats. A

copy of the backups shall be stored in an off-site location for protection against major failure and/ or disaster.

d. A well-defined and documented procedure shall be established for the issuance of the certificates including user request, user credential verification, certificate approval and user undertaking.

e. The user key pair may be generated by the user or by airtel internal CA. It shall be ensured that no copy of the user's private key is retained by the internal CA to avoid risk of repudiation.

f. In order to reduce the likelihood of compromise, the certificates shall have a defined activation and deactivation date, so that they are used only for a limited period of time. airtel as an internal CA shall decide the validity period of the user certificate.

g. In case internal CA's private key is compromised, it is recommended to do the following:-

   i. Warn the users regarding key compromise;

   ii. Revoke all affected user certificates; and

   iii. Change CA private key and reissue the user certificates.

12.5.2 PKI- External Certifying Authority

a. If airtel opts for an external Certifying Authority, it shall be ensured that the following are addressed:-

   i. Trust – The CA is organised, controlled and regulated in such a way that its operations can be relied upon.

   ii. Accreditation - The CA is accredited by a recognised national, regional and international group.

   iii. Compliance – The CA is operating in compliance with accepted industry standards and all relevant regulations.

   iv. Contract – There is a legally binding contract in place covering the provisions of the service and addressing all the issues.

   v. Liability- There is a clear understanding as to the issues of liability. The circumstances under which the CA is liable for damages have been specified. The liability is adequate considering airtel's exposure. The CA has sufficient resources to meet its potential liabilities.

   vi. Security Policy – The CA has a security policy covering technical and administrative requirements.

b. When using the services of an external CA, airtel shall act as the Registration Authority (RA) for its employees. The RA is responsible for validating the credentials of the employees seeking digital certificates and for revocation reporting.

12.6. Key Management

The cryptographic techniques are only effective in supporting security objectives, if keys are securely managed over their lifecycle.

a. The key management procedures for secure key generation, ownership, distribution, archival, storage and revocation shall be established to protect the keys throughout their lifecycle. The procedures shall address following aspects related to key management:-

   i. Key Generation;

   ii. Key Distribution;

   iii. Key Storage;

   iv. Key Change;

   v. Key Destruction;

   vi. Key custodians and requirements for Dual Control;

   vii. Prevention of unauthorised substitution of keys;

   viii. Replacement of known or suspected compromised keys; and

   ix. Key Revocation.

b. The cryptographic keys shall be protected against unauthorised modification, substitution, unintended destruction and loss. The secret keys associated with symmetric cryptographic algorithms and private keys associated with asymmetric cryptosystems shall be protected against unauthorised disclosure.

13. E-mail Security Policy (BISP/Africa – 013)

13.1. 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.

13.1.1 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 airtel are required to adhere to the E-mail Security Policy.

13.2. Policy Statement and Objective

As a productivity enhancement tool, airtel encourages the business use of electronic messaging systems. E-mail security is of prime importance and suitable technological and user level controls shall be implemented to maintain the confidentiality, integrity and availability of the E-mail system.

The objectives of the E-mail policy are to:-

a. Establish the rules for the business use of the E-mail system of airtel and to adequately protect the information transmitted through E-mails; and

b. Ensure that the E-mail system of airtel is not used for malicious activities.

13.2.1 Authorised Use of E-mail

a. All messages generated by the E-mail System are considered to be the property of airtel. 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 airtel.

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.

13.2.2 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 airtel;

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. Forwarding of official E-mails to personal E-mail accounts such as Gmail, Yahoo mail, Hotmail, etc. is prohibited

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

h. Mail-bombing the other users.

13.3. 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)*.

d. Users shall not auto forward their emails to an external email Id.

13.3.1 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.

13.3.2 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.

13.3.3 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 airtel.

13.4. Disclosure of Content

a. Background checks and police verification of all personnel, whether they are airtel employees or Third-party staff, shall be done prior to their appointment as administrators or technical support staff of the E-mail or any other messaging systems. The Third-party staff who are to be assigned such duties shall be approved by HR function of airtel prior to their taking up such assignment.

b. 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.

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

d. 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.

13.4.1 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. They shall keep this document updated.

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

13.4.2 Public Representations

a. No E-mail message related to airtel 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*.

13.5. 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 archived by the users.

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.

13.6. 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.

13.7. Disclaimer

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

13.8. Monitoring and Enforcement

a. The users shall have no expectation of privacy in anything they store, send or receive on the E-mail system. airtel 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*. Failure to comply may result in consequence management.

13.9. Group E-mail ID Management Policy

As per the *E-mail Security Policy* (BISP/Africa – 013), a unique e-mail ID shall be assigned to each user within airtel. 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 airtel 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.

13.9.1 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.

13.9.2 Public Group ID

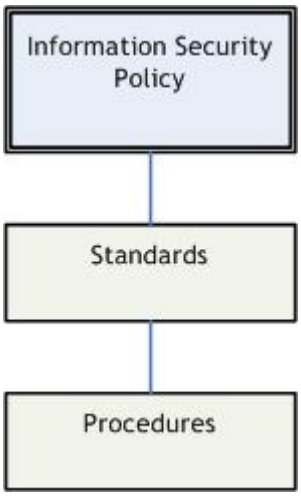
a. An approved list of e-mail IDs that can send e-mails to public group IDs shall be maintained.

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.

14. Information Security Policy Framework



14.1. 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 airtel. 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, Payment Card Industry – Data Security Standard (PCI-DSS) and any other relevant regulations applicable to the OpCo. This policy document supersedes any previous Information Security policy document endorsed by the OpCo.

14.2. Standard

A Standard contains the technical specifications related to a particular control/area. For example, the Cryptographic Standard contains the technical specifications of the various cryptographic algorithms that can be used. Adherence to these standards is a mandatory requirement to safeguard the information assets of airtel.

14.3. Procedures

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

15. Regulatory Compliance

15.1. Introduction

The *Regulatory Compliance Policy* provides the directions to ensure that the business complies with mandated rules and regulations by the Government and their representative bodies in each OpCo.

15.2. Responsibility

The Legal and Regulatory function must collate all information pertaining to rule and regulations stipulated by the Government and their representative bodies as relevant to the operations of Airtel in the respective country. They will disseminate the mandatory conditions imperative for compliance to all concerned functions and a process to enforce this will be promulgated as an annexure to this policy in BISP/Africa. To facilitate the latter, the Legal and Regulatory function will give prompt intimation to the Head of Information Security at airtel for inclusion as an annexure to the BISP/Africa.

All employees of airtel and third party staff are required to adhere to the Regulatory Compliance Policy.

15.3. Policy Statement and Objective

The ability of airtel to do business rests on regulatory compliance. It is therefore imperative for all employees and third party staff to strictly comply with applicable rules and regulations. These may include elements such as KYC, Customer Privacy, Lawful Interception, Remote Access restrictions, etc., varying from country to country.

The objectives of the Regulatory Compliance policy are to:-

a. Establish the procedures necessary to comply with rules and regulations laid down by the Government and their representative bodies as relevant to the operations of Airtel in the respective country.

b. Promulgate the procedures, as an annexure to BISP Africa through Intranet and other means to all stakeholders in the respective OpCos to ensure proactive compliance

c. Establish checks to measure compliance to these laid down procedures of airtel, and enforce appropriate consequence management in case of non-compliance.