Information Security Framework

Version: 2.0

March 2012

Certificate of Approval

Information Security Framework

Version 2.0

(All policy, procedure, guideline, form, manual and template listed in)

Document Title /Name	**Safeguarding of Asset: Information Security Framework**
Document /Policy Number	ISMS/Pol/01
Current Version	2.0
Document/Policy Owner	Chief Technology Officer,
Document Author	Firoz Haider Khan
Approver	Chief Executive officer / Chief Technology Officer, Organization
Effective From	15th March 2012
Next Revision Date	As required
Document Type/Classification	Internal
File Name	Information Security Framework V2.0.docx, MS word 2007
Document /File Location	

Document Amendement Records

A =Added, M = Modified, D = Deleted

Version No.	Date	Section No.	A/M/D	Description	Author
Version 1.0	1st Oct 2010	-	-	1st version.	Firoz Haider Khan
Version 2.0	15th March 2012	Whole Document	A/M	2nd version	Firoz Haider Khan

Information Security Framework Statement

OBJECTIVE

The objective of information security is to ensure business continuity and minimize business damage by preventing and minimizing the impact of security incidents.

NOTES

1. *Information takes many forms and includes data stored on computers+B3, transmitted across networks, printed out or written on paper, sent by fax, stored on tapes and diskettes, or spoken in conversations and over the telephone.*
2. *The protection of valuable or sensitive information from unauthorized disclosure or intelligible interruption.*
3. *Safeguarding the accuracy and completeness of information by protecting against unauthorized modification.*
4. *This applies to record keeping and most controls are already in place; it includes the requirements of legislation such as the Companies Act, the ICT Act, BTRC rules and ISO 27001 controls.*
5. *This ensures that information and the vital services are available to users when they need them.*
6. *This may be a part or full-time role for the allocated person.*

- The purpose of the Framework is to protect the company's information assets like people, physical, software & network asset from all threats, whether internal or external, deliberate or accidental.
- The CTO/CEO has approved the Information Security framework and its Policy listed in section 7.
- It is the framework / Policy of the Company to ensure that:
  - Information will be protected against unauthorized access.
  - Confidentiality of information will be assured.
  - Integrity of information will be maintained.
  - Regulatory legislative and contractual requirements will be met.
  - Business Continuity plans will be produced, maintained and tested.
  - Information security training will be available to all stuff.
  - All breaches of information security, actual or suspected, will be reported to, and investigated by the Information Security Manager.
- Standard will be produced to support the policy. These may include virus control, passwords, encryption and network access control.
- Business requirements for the availability of information and information system will be met.
- The role and responsibility for managing the information security/network security, referred to as the Head of Network Security & Audit, will be performed by: Firoz Haider Khan.
- The Information Security Managerhas direct responsibility for maintaining the Policy and providing advice and guidance on its implementation.
- All managers are directly responsible for implementing the Policy within their business areas, and for adherence by their staff.
- It is the responsibility of each employee to adhere the Framework/Policy.

Table of Contents

1. INTRODUCTION

Information Security Framework establishes security policy and practices for Organization. This framework sets out top management's direction on, and commitment to, information security. It defines information security, staff responsibilities regarding information security and sets out the desired information security behavior for staff.

Policy/procedure general, overarching guidance on matters affecting information security that Organization members are expected to follow.

The foundation for code of practice for information security in Organization is ISO/IEC 27001:2005 and ISO/IEC 27002:2005 has used as guidance for implementation of information security.

2. PURPOSE

The purpose of this procedure is to achieve and maintain confidentiality, integrity and availability of Information and Information Processing Facilities.

This procedure applies to, but is not limited to, safeguarding of the following assets:

- Physical assets (e.g. Network & Telco equipment computer hardware, communication facilities, information processing facilities).
- Information/data (e.g. documents, databases, IT/GSM Systems, Software).
- Organization/Management.
- The ability to provide a product or service.
- People (knowledge, experience, skills).
- Intangibles (e.g., goodwill, image).

3. SCOPE

This security framework shall contribute to the implementation of Information Security in Organization. This framework applies to Organization, including all regular and contractual employees, vendor, consultants, partner and others who are responsible for assets in Organization.

4. DEFINITIONS

- **Information**

Anything of informational value, no matter whether it is in written, digital, oral or other form

- **Information Processing Facilities/ Information System**

Any information processing system, service or infrastructure, or the physical locations housing them

- **Information Security**

All aspects related to defining, achieving and maintaining confidentiality, integrity, availability, authenticity and reliability of information or Information Processing Facilities. Information Security or IT/GSM security team referred as Network Security & Audit team.

- **Information Security Incident**

An Information Security Incident is a single or a series of unwanted or unexpected Information Security Events that have a significant probability of compromising business operations and threatening Information Security.

- **Information Security Event**

  An Information Security Event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a situation that may be security relevant.

- **Information Classification**

  Classification of information in terms of its business critical value, legal requirements and sensitivity like Confidential", "Internal", "Secret", "Open"

- **Information System Class**

  Classification of systems into predefined classes to indicate business criticality, like"Extremely critical", "Critical", "Less critical", "Non-critical"

- **Owner**

  Identifies an individual or Business Unit that has approved management responsibility for a system or controlling the production, development, use, security of the Information

  The term 'owner' does not mean that the person actually has any property rights to the asset

- **Personal Data**

  Any information and assessments that may be linked to a natural person (not corporate body)

  This may be information regarding customers, employees or others, including Personal Data collected by e.g. video surveillance and information from access control systems, customer and employee databases, etc.

- **Telecom Fraud**

  Telecom Fraud is Fraud related to the production and delivery of the telecommunication services, value added services and the necessary infrastructure and support systems for the delivery of such services. Telecom Fraud can affect the customers as well as the company.

5. PROCEDURAL ACTION STEPS

This information Security framework will be considered as guide for implementation of Information Security in Organization.

5.1 Organization and Responsibility

CEO/CTO is responsible for implementation of this procedure within the context of the Business Unit's business activities and risk exposure and to ensure that a consistent and effective approach is applied to management of Information Security of assets.

CEO/CTO will assign an Information Security Head responsible for development and implementation of information security policy/procedure in Organization. She/he is responsible for maintenance, implementation and monitoring of this procedure. This person shall be responsible for the local approach and act as liaison between the Business Unit and the Axiata Group.

5.2 Information Security Procedure (Documents Control)

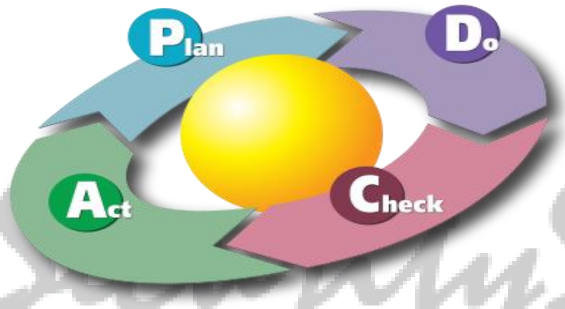
Information Security procedure/ relevant document shall be implemented and maintained. This document should state management commitment and set out the organization's approach to managing information security. All policy documents should contain statements concerning:

a. Approve documents for adequacy prior to issue.
b. Review and update documents as necessary.
c. Ensure that changes and the current version status of documents are identified.
d. Ensure that documents are available to those who need them.
e. Ensure that the distribution of documents is control;
f. Prevent the unintended use of obsolete documents

5.3 Plan-Do-Check-Act Approach

The following steps shall ensure security management in Organization based on a documented Plan-Do-Check-Act process. Plan-Do-Check-Act" (PDCA) cycle helps in analyzing the organization's current state in the cycle.

The plan–do–check–act cycle is a four-step model for carrying out change. Just as a circle has no end, the PDCA cycle should be repeated again and again for continuous improvement.



Information security responsible will ensure the following steps to ensure information security management in Organization:

a. Understand Organization information security requirements and develop policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.
b. Implement and operate the policy, controls, processes and procedures
c. Monitor and review the performance and effectiveness of the management of information security ; and
d. Take corrective and preventive actions, based on the results of the internal audit and management review or other relevant information, to achieve continual improvement.

5.4 Information Security Incident Management Procedure

Organization will maintain a Security Incident management procedure to ensure that Information Security events and weaknesses associated with Information processing facilities are communicated in a manner allowing timely corrective action to be taken. Documents shall be in place to ensure that any significant event is reported, logged and collected for analysis. Policy/Procedures shall assure incident investigations are complete and minimize further damage.

Organization will communicate information security incidents through documenting events, identifying the scope of the incident, and notification of owners of impacted information or assets. Security incidents shall be reported in a timely manner.

5.5 Information and Information System Classification & Protection

Organization will maintain a guideline for information and information system classification & protection. Information will be classified in terms of its business critical value, legal requirements and sensitivity.

Information System shall be classified to ensure that the business value and the overall importance of an information system is recognized.

All Information Systems shall be classified into one of four categories, as described in the template for Classification of Information Systems:

- **Category A:** Extremely critical and important systems
- **Category B:** Critical and important systems
- **Category C:** Less critical and important systems
- **Category D:** Non-critical systems

The Information Protection policy aims at establishing a common understanding and approach to information security so to ensure better compliance by all concerned parties.

5.6 Software Development and Maintenance

Organization shall identify and design security requirements in the business process of developing applications and user-developed applications.

Organization shall develop applications with secure code and develop secure code through established standards, conductive development environments and methodologies. Contract provisions for third-party application developments should provide enforceable and effective protection regarding application security.

Appropriate controls should be designed into applications, including user developed applications to ensure correct processing and right access to information. These controls should include the validation of input data, internal processing and output data.

5.7 Human Resources Security

5.7.1 Termination or Change of Employment

To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner.

5.7.2 Termination Responsibilities

Responsibilities for performing employment termination or change of employment shall be clearly defined and assigned.

5.7.3 Return on Assets

All employees, contractors and third party users shall return all of the organization's information assets in their possession upon termination of their employment, contract or agreement.

5.7.4 Removal of Access Right

The access rights of all employees, contractors and third party users to information and information processing facilities must be removed upon termination of their employment, contract or agreement, or adjusted upon change.

5.7.5 Disciplinary Process

There should be a formal disciplinary process for employees who have committed a security breach. Any employee found to have violated this policy may be subjected to disciplinary action will be handled via existing organization governing bodies and procedures. In serious cases of misconduct the process should allow for instant removal of duties, access rights and privileges and for immediate escorting out of the site, if necessary.

5.8 Information Security Risk Assessment and Treatment

Information risk is the chance or possibility of harm being caused to a business as a result of a loss of the confidentiality, integrity or availability of information. A process approach for assessing risks, treating risks and ongoing risk monitoring, risk reviews and re-assessments plans shall be documented.

The risk assessment process shall cover a selection of processes and systems for assessment. The risk assessment process for information systems shall take system class and processing of personal data into consideration.

5.9 Access Control

Access to information and Information Processing Facilities shall be controlled on the basis of business and security requirements. Users shall only have access to the information and resources that they have been specifically authorized to use.

The allocation of privileges shall be controlled through a formal and documented authorization process.

Organization shall require each workforce member to have a unique ID with Information Resources access limited only to authorized users subject to defined limitations

Special or administrator privileges shall be granted only to workforce members needing them to complete their duties and this number shall limited to the minimum number possible without compromising service levels. Administrative privilege must be justified and approved. Segregation of duties shall be applied for personnel with extensive system privileges. C-level, EVP and Head of Network & Security will avail local administrative privilege by default.

If possible all system administrator and system management activities shall be logged.

5.10 Security Education

Security education, training, and awareness program shall be in place to ensure related resources and end-users are aware of the security issues and their implications. Employee (user) should be made aware of the key elements of the information security and why it is needed and understand their personal security responsibilities.

Head of Information Security/ Head of Network Security & Audit will arrange special information security implementation training for key relevant employees or system administrators.

6. ACTION STEPS TO MAKE THE PROCEDURE EFFECTIVE

6.1 Communication, Understanding and Support

This security framework or relevant documents will be available on the local intranet under the heading Information Security Policy & Procedure. Head of Network Security & audit is responsible to maintaining this procedure is effective.

Information Security framework, awareness shall be communicated effectively to the employees through the use of Organization's intranet and other relevant means, including email and SMS distribution.

6.2 Monitoring, Compliance and Security Audit/Review

The security condition of Organization should be monitored regularly. Security monitoring arrangement provides key decision–makers with an informed view of the effectiveness and efficiency of information security arrangements and the area where improvement is required.

Information security - Organization may conduct a third party review on need basis to check the objectives and controls set by Information Security Procedure are properly carried out.

Head of Information Security/Head of Network Security & audit will ensure access to data collected in Intrusion Detection Systems (IDS/IPS), IDM, log management system, SCCM, application manager or any other monitoring devices/tools within or in direct connection with the Business Unit's Information Processing Facilities. Head of security and his/her nominated personnel will avail all necessary tools, administrative privilege and full access in all tools, system, application and database by default.

Information system and application logged file will be maintain and review as per need basis.

7. POLICY AND PROCEDURES

Following policy / procedure /template will be used as part of this security framework to ensure to the integrity, confidentiality and availability of resources of Organization of Bangladesh.

SL	Policy / Procedure	Document #	Purpose	Target Employee
1.	Acceptable Use Policy	ISMS/Pol/002	The purpose of this policy is to outline the acceptable use of computer equipment at Company	All Employees
2.	Access control policy	ISMS/Pol/003	This document defines the access control policy required to securely deploy, manage and control user network, operating system, application and database access.	Group of Employee. System/Application Owner
3.	Antivirus policy	ISMS/Pol/004	To establish requirements which must be met by all computers connected to Company's networks to ensure effective virus detection and prevention.	All Employee
4.	Backup policy	ISMS/Pol/005	This policy establishes a backup strategy to address different types of service disruptions; minimal backup frequencies; recovery point objectives; and establishes the roles of various Staff positions having responsibilities relating to backup and recovery of critical systems and services.	Authorized Group of Employee. Backup Team.

5.	Data Centre Access Policy	ISMS/Pol/006	The purpose of this policy is to provide guidelines how Company individuals will conduct themselves within the Datacenter.	Authorized Employee. Not for all
6.	Database Security Policy	ISMS/Pol/007	This policy states the requirements for securely storing and retrieving database usernames and passwords (i.e., database credentials) for use by a program that will access a database as well as overall database administration security for any Database running on of Company's networks.	Database Team, Authorized Employee.
7.	E-mail policy	ISMS/Pol/008	The purpose of the policy is to ensure that we use the email system in an efficient but at the same time careful way when we communicate.	All Employee
8.	Encryption Policy	ISMS/Pol/009	The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively.	All Employee
9.	Information protection policy	ISMS/Pol/010	The Information Protection Policy aims at establishing a common understanding and approach to information security so to ensure better compliance by all concerned parties.	All Employee
SL	**Policy / Procedure**	**Document #**	**Purpose**	**Target Employee**
10.	IT Policy	ISMS/Pol/011	The purpose of this IT policy is to address all issues relevant to standardization of hardware equipment and application software, software installation, deployment, access and security of IT/Technology resources in Organization.	All Employee

11.	Information Classification policy	ISMS/Pol/012	The Information Classification Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of Organization without proper authorization.	All Employee
12.	Internet DMZ Security Policy	ISMS/Pol/013	The purpose of this policy is to define standards to be met by all equipment owned and/or operated by Company located outside Company's corporate Internet firewalls.	Authorized Employee. Not for all.
13.	Internet usage policy	ISMS/Pol/014	Rules for Internet use	All Employee
14.	Intrusion Detection Policy	ISMS/Pol/015	It provides guidelines about intrusion detection implementation of the organizational networks and hosts along with associated roles and responsibilities.	Authorized Employee
15.	Log monitoring policy	ISMS/Pol/016	This policy reflects the Company's commitment to identify and implement security controls to keep risks to information system resources at reasonable and appropriate levels.	Authorized Employee
16.	Media disposal policy	ISMS/Pol/017	This policy defines the steps necessary to implement Company's information system & media disposal.	All Employee
17.	End-user Password policy	ISMS/Pol/018	The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.	All Employee
18.	Patch management policy	ISMS/Pol/019	This will guide Windows OS patch update for Windows 2003 Enterprise Server R2	Windows Team
SL	**Policy / Procedure**	**Document #**	**Purpose**	**Target Employee**

19.	Personal Computer Security Policy	ISMS/Pol/020	The purpose of this policy is to establish standards for the base configuration of internal Desktop equipment (PC/Laptop/Printer) that is owned and/or operated by Company.	All Employee
20.	Remote access policy	ISMS/Pol/021	The purpose of this Policy is to define standards for connecting to Company's network from any remote host, untrusted host, and remote network, including untrusted hosts on Company's intranet.	All Employee
21.	Information Security risks treatment policy	ISMS/Pol/022	This policy acknowledges that once risks are identified they must be treated.	All Employee
22.	Information Security risk assessment policy	ISMS/Pol/023	This policy stresses the importance of conducting risk assessments on Information Resources.	All Employee
23.	Router Security Policy	ISMS/Pol/024	This document describes a required minimal security configuration for all routers, switches and others perimeter devices connecting to a production network or used in a production capacity at or on behalf of Organization.	Authorized Employee
24.	Server Security Policy	ISMS/Pol/025	The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by Company.	Authorized Employee
25.	Third party access control policy	ISMS/Pol/026	The aim of this third party access security policy is to allow the Company to exploit the business benefits of third party access in a secure manner and to manage the associated risks effectively.	All Employee
26.	Virtual Private Network (VPN) Policy	ISMS/Pol/027	The purpose of this policy is to provide guidelines for Remote Access IPSec or L2TP Virtual Private Network (VPN) connections to the Organization corporate network.	VPN User Group, All Employee

SL	Policy / Procedure	Document #	Purpose	Target Employee
27.	Wireless Communication Policy	ISMS/Pol/028	This policy describes how wireless network communication technologies are to be deployed, administered, and supported at Organization.	All Employee
28.	General & Miscellaneous Policy	ISMS/Pol/029	This will give idea General rules for handling IT resources	All Employee
29.	Laptop policy	ISMS/Pol/030	Rules for Laptop	All Employee
30.	Software Acquisition Policy	ISMS/Pol/031	The purpose of this document is to outline the steps that Company need to take in order to ensure that all purchase software is processed into inventory tracking process/system and all documentation of ownership is properly stored and maintained and copy right low follows.	All Employee
31.	File Serve Policy	ISMS/Pro/032	The purpose of this policy is to protect the company's information/data from all threat whether internal or external, deliberate or accidental. The file server policy aims at establishing a common understanding and approach to file server so to ensure better data/file management, compliance by all concerned parties.	All Employee
32.	Internal Audit Procedure	ISMS/Pro/001	This document provides guidelines and procedures for internal audit of ISMS.	Technology Audit Team
33.	Procedure for corrective and preventive action	ISMS/Pro/002	Provides detailed procedures for implementation of preventive and corrective actions for information security incident or any non-conformance encountered during internal audit / external audit process.	Technology Audit Team
34.	Procedure for protection and Control Document	ISMS/Pro/003	This is the procedure, identified in section 5.2 of the Organization's information security framework/ policy, for defining how the Organization protects and controls the documents required by the ISMS.	Technology Audit Team

35.	Change Management Process and Strategy	ISMS/Pro/004	Change Management procedure.	All Employee
SL	**Policy / Procedure**	**Document #**	**Purpose**	**Target Employee**
36.	Information Security Incident Handling Procedure	ISMS/Pro/005	The document provides some general guidelines and procedures for dealing with IT / Technology incidents.	All Employee
37.	Information Security Risk Management Methodology	ISMS/Pro/006	The purpose of the risk assessment is to identify all susceptibilities to the identified threats, and the nature of the harm that could arise from them.	All Employee
38.	Procedure for Router Security	ISMS/Pro/007	Essential security configuration for router.	Authorized User
39.	Information security awareness training manual	ISMS/Man/001	Information Security Awareness Manual	All Employee
40.	Security Guideline for Project	ISMS/GUI/001	The purpose of these guidelines is to ensure that appropriate level of information security control is in place for new business initiatives/project.	Project Team, Authorized Employee
41.	Information Security Incident Handling Form	ISMS/For/001	Report Form	All Employee
42.	System Classification procedure	ISMS/Pro/008	System Classification procedure	All Employee
43.	Software development life cycle	ISMS/Pro/009	Software development guideline	Development Team
44.	Core Site Physical Access Guidelines	ISMS/Gui/003	This policy aims at providing protection of all Organization assets, business processes and employees	Authorized User

			from external and internal theft, accidental or malicious damage, sabotage, subversion, leakage and other natural threats by establishing cost effective security solutions	

8. REFERENCES

[1] ISO/IEC 27002:2005 Information technology -- Security techniques -- Code of practice for information security management [ISO 27002]

[2] ISO /IEC 27001:2005 Information Technology – Security techniques –Information security management systems – Requirements.