INFORMATION SECURITY POLICY

**Author Signature Date**

|  |  |  |
| --- | --- | --- |
|  |  |  |

**Reviewed By:**

**Name Signature Date**

|  |  |  |
| --- | --- | --- |
|  |  |  |
|
|

**Approved By:**

**Name Signature Date**

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |

**Document Ownership**

Information Security

**Document Control**

The validity of this document is limited to the use of the policy as a guideline for Information Security XXXX-wide. In the event that the adopted policy framework changes, the document will have to be reviewed and the document owner must assess this document for relevancy at that point. This document will be reviewed at least annually and updated accordingly to reflect changes to business objectives or the risk environment.

**Distribution Control**

The Document Owner controls distribution of this document. The distribution is as follows:

* Chief Information Security Officer
* Chief Information Officer
* Chief Risk Officer
* Chief Audit Executive
* Chief Compliance Officer
* Head, Human Capital Management

**Notice and Warning**

Copyright©2019, XXXX.

This document is the property of XXXX; 54, Marina Street, Lagos. Circulation is restricted to the XXXX’s use. It must not be copied or used for any other purpose other than which it is supplied, without the expressed written authority of XXXX.

Except where provided for purposes of contractual requirements, XXXX. disclaims any responsibility or liability for any use or misuse of the document by any person and makes no warranty as to the accuracy or suitability of the information to any third party. Any misuse of the document is addressable by XXXX.

**Summary**

This Information Security Policy explains why Information Security is important to XXXX. It provides a single point of reference for the XXXX information security related policies, guidelines and procedures.

CONTENTS

1. INFORMATION SECURITY POLICY 7

[1.1 INTRODUCTION 7](#_Toc19197702)

[1.2 PURPOSE 7](#_Toc19197703)

[1.3 SCOPE 7](#_Toc19197704)

[1.4 DEFINITIONS 8](#_Toc19197705)

[1.5 OBJECTIVES 8](#_Toc19197706)

[1.6 RISKS 8](#_Toc19197707)

[1.7 RESPONSIBILITIES 8](#_Toc19197708)

[1.8 STATEMENT 11](#_Toc19197709)

[1.9 RISK MANAGEMENT 11](#_Toc19197710)

[1.10 INCIDENT RESPONSE PLAN 12](#_Toc19197711)

[1.11 COMPLIANCE (LEGAL, REGULATORY AND CONTRACTUAL) 13](#_Toc19197712)

[2.1 Information Classification and Control Policy 14](#_Toc19197713)

[2.2 Physical Asset and Control Policy 19](#_Toc19197714)

[2.3 Asset Inventory Policy 21](#_Toc19197715)

[2.4 Data Retention Policy 23](#_Toc19197716)

[2.5 Information Disposal Policy 27](#_Toc19197717)

[**2.6** **System Documentation Policy** 30](#_Toc19197718)

[2.7 Acceptable Use Policy 31](#_Toc19197719)

[2.8 Access Control Policy 35](#_Toc19197720)

[2.9 Human Resources Security Policy 39](#_Toc19197721)

[2.10 Password Policy 42](#_Toc19197722)

[**2.11** **E-mail Security Policy** 45](#_Toc19197723)

[**2.12** **Internet Usage Policy** 49](#_Toc19197724)

[**2.13** **Security Awareness and Training Policy** 52](#_Toc19197725)

[**2.14** **Clear Desk & Clear Screen Policy** 53](#_Toc19197726)

[**2.15** **Physical and Environmental Security Policy** 56](#_Toc19197727)

[**2.16** **Third Party Access Policy** 59](#_Toc19197728)

[**2.17** **Remote Access Policy** 62](#_Toc19197729)

[**2.18** **Malware & Antivirus Policy** 64](#_Toc19197730)

[**2.19** **Vulnerability Management Policy** 68](#_Toc19197731)

[**2.20** **Information Security Incident Management Policy** 72](#_Toc19197732)

[2.21 Backup and Recovery Policy 79](#_Toc19197733)

[2.22 Business Continuity Policy 79](#_Toc19197734)

[2.23 Cryptography Policy 81](#_Toc19197735)

[2.24 Supplier Control Policy 84](#_Toc19197736)

[2.25 Information Transfer Policy 86](#_Toc19197737)

[2.26 Risk Assessment Policy 88](#_Toc19197738)

[2.27 Media Transportation Policy 92](#_Toc19197739)

[2.28 Mobile Device Policy 93](#_Toc19197740)

[**2.29** **Communications Policy** 95](#_Toc19197741)

[2.30 Software Management Policy 97](#_Toc19197742)

[2.31 Hardware Management 100](#_Toc19197743)

[2.32 Access to Operating System Software 101](#_Toc19197744)

[2.33 Data Governance Policy 102](#_Toc19197745)

[2.34 Social Media Policy 106](#_Toc19197746)

[2.35 Wi-Fi Acceptable Use Policy 107](#_Toc19197747)

[2.36 CCTV Policy 110](#_Toc19197748)

[2.37 Bring Your Own Device (BYOD) Policy 112](#_Toc19197749)

[2.38 Log Management Policy 115](#_Toc19197750)

[2.38.1 Introduction 115](#_Toc19197751)

[2.38.2 Purpose 115](#_Toc19197752)

[2.38.3 Scope 115](#_Toc19197753)

[2.28.4 Objective 115](#_Toc19197754)

[2.38.5 Roles and Responsibilities 115](#_Toc19197755)

[2.38.6 Policy Details 115](#_Toc19197756)

[3. ENFORCEMENT 118](#_Toc19197757)

[4. CONTROLS 118](#_Toc19197758)

[5. KEY PERFORMANCE MEASURES 118](#_Toc19197759)

[6. REFERENCES 118](#_Toc19197760)

[7. REVISION HISTORY 118](#_Toc19197761)

# 1. INFORMATION SECURITY POLICY

## 1.1 INTRODUCTION

Information security aims to protect information and information assets and ensure business continuity by preventing and minimizing the impact of information security incidents. Information security provides the trusted environment that the XXXX needs to be confident in adopting efficient new ways of doing business. Information security deals with all aspects of information (spoken, written, printed, electronic or any other medium) and information handling (created, viewed, transported, stored or destroyed).

Information will be classified and protected in a manner commensurate with its sensitivity, value and criticality. Protection of information will apply regardless of the media where the information is stored, the systems that process it, or the transport mechanisms by which it is moved. XXXX. will seek to enhance productivity of the business by reducing the probability of loss through the design and implementation of policies, standards, procedures and guidelines that enhance the protection of business assets.

There are three basic elements to information security that must be maintained at all times to protect against loss, damage and unauthorized disclosure of information:

* Confidentiality: protecting sensitive information from unauthorized disclosure or interception.
* Integrity: safeguarding the accuracy and completeness of information and computer software.
* Availability: process of ensuring that authorized users have access to information and associated assets when required.

## 1.2 PURPOSE

The purpose of this policy is to define the requirements for information security within XXXX., define roles and responsibilities, to provide direction for the board and senior management and establish high-level guiding principles for information security in accordance with business requirements, relevant laws and regulations, and contractual requirements.

## 1.3 SCOPE

This document applies and is of importance to all employees of the XXXX, including temporary Staff, external partners/vendors and contractor personnel and other third parties. Conformance to the Information Security Policy is therefore required from the moment an employee or third parties joins or works for XXXX. until the moment he/she leaves.

The scope of this Information Security Policy includes, but is not limited to:

* All information processed by the XXXX in pursuit of all its operational activities, regardless of whether it is processed electronically or in paper form, including but not limited to:
  + Customer information
  + Operational plans, documents and records
  + Employee records
* All information processing facilities used in support of the XXXX’s operational activities to store, process and transmit Information
* All external organizations that provide services to the XXXX in respect of information processing facilities

All users must understand and adopt use of this policy and are responsible for ensuring the safety and security of the XXXX’s Information and Information assets. Violations of this policy will be documented and can lead to revocation of system privileges and/or disciplinary action up to and including termination.

## DEFINITIONS

* **The XXXX:** This refers to XXXX.
* **Third parties**: include contractors, vendors, external auditors, consultants and any other person who is not an employee of the XXXX.
* **Users:** is a term inclusive of all employees of the XXXX, including temporary Staff, external partners/vendors and contractor personnel and other third parties.
* **Information Asset** – Any information and information processing assets of value to the XXXX.
* **Information Owner** – individual accountable for the Information Asset
* **PCI-DSS** – Payment Card Industry Data Security Standard – regulations surrounding how cardholder data is stored, processed and transmitted.
* **R** = **Responsible** = The user who does the work to achieve the task
* **A** = **Accountable** = The user ultimately accountable for the task or decision being made
* **C** = **Consulted** = The user who must be consulted prior to a decision being made and/or the task being completed
* **I** = **Informed** = The user who must be told when a decision is made, or work is completed

## 1.5 OBJECTIVES

The objective of the Information Security Policy is to protect the XXXX’s information assets from accidental or intentional loss, disclosure, attack or misuse. All reasonable measures shall be taken to ensure that:

* The XXXX’s information remains confidential
* The integrity of information is maintained
* The XXXX’s requirements for the availability of information and the systems used to process information are met
* Accountability for information is maintained
* All appropriate regulatory and legislative requirements are met in full

The Information Security Policy sets out supporting policies and standards intended to help the XXXX achieve these objectives.

Compliance with this Information Security Policy is necessary to ensure business continuity, and minimise business damage by preventing the occurrence, and minimising the impact, of information security incidents.

Breaches of the Information Security Policy and any supporting policies or standards, or who knowingly or negligently allows employees or contractors under their supervision to do so will be subject to disciplinary action and up to termination of employment.

## 1.6 RISKS

Lack of, or failures in, information security can lead to incidents such as breach of the confidentiality of information, damage to its integrity, or issues surrounding its availability, which could lead to direct financial loss, damage to the XXXX's reputation and/or breach of regulatory standards or the law.

## 1.7 RESPONSIBILITIES

1. The Board of Directors has oversight and overall responsibility for the XXXX’s Information Security Office. Responsibilities include:

* Provide leadership and direction for effective conduct of the processes.
* Ensure that information security governance is integrated into the XXXX’s structure and relevant processes.
* Ensure that information security processes are conducted in line with business requirements; applicable laws and regulations while ensuring security expectations are defined and met across the XXXX.
* Ensure that the audit function of the information security processes is independent, effective and comprehensive.
* Be responsible for all information security governance documents such as information security strategy, framework and policies and ensure alignment with the overall business goals and objectives.
* Receive and review reports submitted by senior management that details the overall status of the information security programme to ensure that Board - approved risk thresholds relating to information security are being adhered to.
* Ensure that the information security budget is approved.

1. The XXXX’s senior management shall be accountable for:

* Implementation of the Board-approved information security policies, standards and the delineation of information security responsibilities.
* Provision of periodic reports (at a minimum quarterly); to the Board on the overall status of the information security programme of the XXXX.
* Managing and reducing risk in an informed manner.
* Minimizing the impact on the XXXX when information security incidents occur.
* Ensuring that appropriate security and legal controls are identified, implemented and maintained by information owners and fully complied with.
* They shall be supported in this task by the XXXX’s Management Risk Committee (MRC), the XXXX’s Information Security function.

1. The XXXX’s Chief Information Security Officer has the direct responsibility for the development and implementation of the information security programme and strategy as approved by the Board. Other responsibilities include:

* Maintaining the Information Security Policy and providing advice and guidance on its implementation.
* Responsible for the day-to-day cyber security activities and the mitigation of cyber security risks in the XXXX.
* Focus on the XXXX’s cyber security risk rather than IT security risk only.

1. The responsibility for managing information security at an operational level shall be performed by the XXXX’s Information Security Team. This team is responsible for:

* Setting and maintaining, documenting and distributing information security standards and policies
* Providing advice and guidance on information security
* Routine monitoring of the status of security within the XXXX
* Recommending and implementing suitable protective measures
* Performing security assessments
* Monitoring, investigating and analysing security breaches
* Ensuring staff receive on-going training and awareness in information security
* Undertaking an annual review of this policy, considering all of the following:
  + Feedback from other areas of the XXXX
  + Results of independent reviews and audits
  + Changes to the business model of the XXXX
  + Trends relating to threats and vulnerabilities
  + Reported information security incidents
  + Recommendations made by relevant authorities
* Undertaking regular reviews of the wording of confidentiality and non-disclosure agreements/clauses to ensure that they:
  + Fully comply with all XXXX agreed policies and standards
  + Take into account any feedback from other areas of the XXXX, the results of independent reviews and audits, any changes to the business model of the XXXX and any recommendations made by relevant authorities
  + Comply with all relevant laws and regulations

1. Other functional responsibilities include:

* Operational Risk Management: Independently evaluates all the risks relating to information security in a proactive way using appropriate tools and methodologies for risk identification, analysis and control. Appropriate reports shall be provided to Senior Management and the XXXX’s Management Risk Committee
* Compliance & Conduct: Has responsibility for monitoring compliance with the policies and the review of information security policies and processes to ensure adherence to relevant CBN directives and other extant regulations.
* Human Capital Management: Employee selection, induction, training and exit-processing
* IS Audit: Ensuring policy compliance and investigation of deviations from policy - specified behaviour, providing assurance to the Board and Senior Management on the effectiveness of the information security policies and processes, ensuring the effectiveness of the controls put in place and ascertaining if they are adequate for the XXXX’s risk exposure.

1. Information Owners within the XXXX shall be responsible for the identification, implementation and maintenance of controls that are commensurate with the value of the information assets they own and the risks to which they are exposed. This information includes:

* Information stored by the XXXX
* Information processed by the XXXX
* Information obtained from external sources
* The XXXX's information when sent to, stored or processed by a third party

1. Managers are responsible for maintaining information security and for enforcing the terms of the Information Security Policy in their areas and amongst the people and/or the external relationships they manage.
2. All employees/users and authorised users are responsible for complying with the Information Security Policy and maintaining an appropriate level of information security. Users must report any security weakness or vulnerability and must not attempt to prove or exploit it. Users must complete all mandatory information security training.

## 1.8 STATEMENT

The XXXX shall ensure that:

* Information assets and information processing facilities shall be protected against unauthorised access
* Information shall be protected from unauthorised disclosure
* Confidentiality of information assets shall be a high priority
* Integrity of information shall be maintained
* The XXXX’s requirements, as identified by information owners, for the availability of information assets and information processing facilities required for operational activities shall be met
* Statutory, and expressed and implied legal obligations shall be met
* Business continuity plans shall be produced, maintained and tested
* Unauthorised use of information assets and information processing facilities shall be prohibited;
* Obscene, offensive, or damaging statements shall be dealt with in accordance with other policies published by the XXXX
* This Information Security Policy shall be communicated to all users for whom information security training shall be given.
* All breaches of information security, actual or suspected, shall be reported and investigated in line with the XXXX’s published policies.
* Controls shall be commensurate with the risks faced by the XXXX. In support of this Information Security Policy, more detailed security policies, processes, and standards shall be developed.

## 1.9 RISK MANAGEMENT

A systematic approach to information security risk management is necessary to identify business needs regarding information security requirements (including contractual and regulatory) and to create an effective operational security framework.

Information security risk management is not a one-off exercise with a single set of control recommendations, which remain static in time, but a continual process. During the operational delivery and maintenance of the XXXX’s products and services there are several instances where risk assessment is necessary.

The implementation of the information risk strategy shall be based on formal methods for risk assessment, risk measurement, risk mitigation/treatment, risk acceptance and risk monitoring and reporting and shall be independent of technology or software.

**Information Security Risk Assessment Process**

* In order to identify key risks, determine and implement appropriate controls, keep those risks within acceptable limits and to measure compliance with the Information Security Policy, annual risk assessments of key XXXX’s environment, departments, systems and processes shall be undertaken upon significant changes to the environment.
* Information security risk assessments shall be performed in conjunction with the business, system or information owner at regular intervals by evaluating all identifiable vulnerabilities; threats and likelihood of successful exploit; potential impact (reputational, financial, regulatory, etc.); and the associated risks in order to estimate the amount of assets and efforts required to recover from losses/damage attributable to potential information security incidents. A documented and agreed assessment process shall be followed.
* Risk assessments should be updated regularly to address changes or introduction of new technologies, products etc. before deployment to ensure accurate risk measurement.
* The assessment should include but not limited to adequacy of information security governance; policies, procedures and standards; inherent risks in business operations; visibility to emerging threats to information assets; capability to swiftly respond and recover from cyber-incidents; vendor risk, and efficacy of existing controls to mitigate the identified risks.
* Development of detailed roadmap that states the risk treatment plan with stipulated time frame to timely address gaps identified.
* Information security risk assessments will specifically focus on risks to the confidentiality, integrity and availability of information.

**Assessment Criteria**

Information security risk assessments will aim to:

* Define the criticality of the environment, department, system or process
* Identify deliberate or accidental threats to the confidentiality, integrity or availability of information stored in or processed by the environment, department, system or process
* Identify critical threats, assets and vulnerabilities
* Assess vulnerabilities due to control weaknesses and special circumstances that highlight vulnerabilities
* Evaluate the likelihood and business impact of threats materializing
* Make recommendations about suitable levels of target control maturity

Information security risk assessments shall be performed as part of the process to implement a change, and on an annual basis.

**Risk Treatment and Risk Reporting**

* Risk treatment options such as risk reduction, risk retention, risk avoidance, risk transfer and how residual risk is addressed should be selected based on the outcome of the risk assessment.
* The results of information security risk assessments, including any forward action and acceptance of any residual risk, shall be reported to the Senior Management and the Board of Directors to support informed decision making.

**Risk Acceptance**

* In some circumstances, it may be appropriate to accept an identified risk or an on-going, long-term digression from Information Security Policy as a legitimate business risk.
* In such cases, upon completion of the information security risk assessment undertaken, the type of systems, information or processes involved will be examined and the implications of accepting the risk assessed.
* XXXX’s Operational Risk Management Team will hold details of accepted risks. Accepted risks will be reviewed for appropriateness on a periodic basis.

## 1.10 INCIDENT RESPONSE PLAN

* In order to immediately respond to an incident involving the security of information, an Incident Response Plan shall be in place. The plan shall contain key elements to allow the XXXX to respond effectively in the event of a breach that could impact on customer information, including cardholder data. The Incident Response Plan shall be tested on an annual basis.
* Designated personnel shall be available on a 24/7 basis to respond to alerts.

## 1.11 COMPLIANCE (LEGAL, REGULATORY AND CONTRACTUAL)

* The XXXX’s legal and regulatory obligations are identified and managed by Legal department.
* It is to be noted that compliance with this policy is a mandatory requirement for all users. Violation of the policy could expose the XXXX to significant legal and business risks, which could be detrimental to the overall achievement of its business objectives. Violations of the policy will be documented and can lead to revocation of system privileges and/or disciplinary action up to and including termination.

### Information Classification and Control Policy

**2.1.1** **Overview**

In order to preserve the appropriate confidentiality, integrity and availability of XXXX’s information assets, the XXXX must make sure they are protected against unauthorized access, disclosure or modification. Different types of information require different security measures depending upon their sensitivity. The XXXX's information classification and control policy is designed to provide information owners with guidance on how to classify information assets properly and then use them accordingly.

* + 1. **Purpose**

To establish guidelines and procedures for managing access and classification of XXXX’s information assets.

**2.1.3 Objectives**

The objective of this document is to provide a rigorous and consistent classification and control system which ensures that information assets are identified, properly classified and are protected throughout the XXXX, in accordance to the XXXX policies and legal requirements.

**2.1.4 Policy Details**

* Access to all information held by the XXXX shall be granted on a need-to-know and need-to-use basis.
* The Information owner shall be taken as the originator of the information or the application owner that produces, stores or processes the information.
* Information owners shall review allocated classifications on a periodic basis to ensure consistency with business and contractual/shareholder/-customer requirements.
* The classification of information and systems shall determine the level of security that will be applied to protect it.
* Systems shall be classified according to the total value of information that they support. All information held by the XXXX shall be classified in one of the four categories below:

1. **CONFIDENTIAL -** This will be applied to information that could extensively damage or be detrimental to the XXXX, its employees or its customers if it is lost, disclosed or modified. This includes information which, if compromised, could negatively affect the effectiveness of management or breach confidentiality agreements. Only a very small amount of the XXXX's information will fall into this category. Confidential documents will normally contain information which, if compromised, could:

* Place employees at risk,
* Influence the share price of the XXXX and/or other companies,
* Prejudice management strategy,
* Adversely affect the XXXX's reputation,
* Cause the XXXX serious financial loss or
* Prejudice litigation.

1. **PRIVATE -** This refers to restricted information and cannot be accessed or released to persons not authorized. Only employees authorized either in roles or positions in the respective departments can access information classified as Private. Information classified as Private also applies to information which, if disclosed, may breach personal privacy and technical controls. Included in this category are employee records, customer personally identifiable information, audit log and tools.
2. **INTERNAL -**  This refers to information not intended to be disclosed outside the XXXX. Information that does not justify a classification of “Internal” will be covered by the oath of secrecy taken by each staff; this information will be accorded reasonable protection to prevent access by third parties.
3. **PUBLIC** -Information that may be released to the public, that does not benefit a competitor, negatively impacts the XXXX or does not breach any confidentiality. XXXX brochures and advertisements fall into this category.

|  |  |  |  |
| --- | --- | --- | --- |
| **CLASSIFICATION** | **LABELLING** | **HANDLING** | **EXAMPLES** |
| **Confidential**   * High Value * Strict Legal Requirements * High Sensitivity * High Criticality to the organization | Confidential | * Confidential refers to the most sensitive business information * Information is restricted to be seen and handled by nominated personnel only * All information in this category should be labelled as Confidential * Confidentiality of this information shall be maintained at the highest level * Password protect information * As removable media is not to be used, no confidential information should be stored on removable media * Destroy any printouts * Do not discuss in public * Do not transmit via email | * Trade secrets * Card Holder Data * Customer information * Core XXXXing Application (and supporting systems) Information * Financial statements * Business design principles * Strategic plans * Intellectual property of the XXXX * Passwords, ATM PIN * Security parameters * Software license key * Authorization codes * Audit Report * Merger and acquisition plans, etc. |
| **Private** | Private | * Information that cannot be released to any persons outside of the restricted permissions set * As removable media is not to be used, no private information should be stored on removable media * Destroy any printouts * Do not discuss in public * Only transmit via email with approval and encryption in place. * Shred all paper copies | * Employee personal records (HCM Files) * Customer personally identifiable information * Project documents * Operational reports of various departments * Audit tools and software, software logs * System documentation and organizational records |
| **Internal** | Internal | * Information that cannot be released to any person outside of XXXX without approval * All XXXX personnel have access to internal information with the permissions that have been set on the XXXX’s IT system. | * Policy manuals * Standard operating procedures * Internal circulars * Internal correspondence and memos * XXXX's telephone directory * Training materials * Intranet / web portals, etc. |
| **Public**  Low Value  Few Legal Requirements  Low Sensitivity  Low Criticality to the organization | Public | * Information that may be released to the public, that does not benefit a competitor, negatively impact XXXX or does not breach any confidentiality. * Information that may be published in any public forum without constraints either enforced by law or discretionary. * By default all information is classified as Public unless otherwise classified. | * Service brochures * Advertisements * Job opening announcements * Press releases * Declared/published financial results etc. |

**Electronic Information Access Matrix**

| **Classification / Access level** | **Staff** | **Vendors** | **Third Parties** |
| --- | --- | --- | --- |
| **Confidential** | * Information Owners. * Executive management and SBU Heads. | Except on legal advice. | Except on legal advice. |
| **Private** | * Information owners. * Information processors within the scope of their function. * Subject of information. | Where duly signed NDA exits. | Except on legal advice. |
| **Internal** | Full Access | Where duly signed NDA exits. | Except on legal advice. |
| **Public** | Full Access | Full Access | Full Access |

Using the matrix above as a guide, access to the following publicly available information on Infoshare access shall be granted as follows:

1. **Staff Accounts**:

Classified as private; access to be restricted to Account Holder, Operations / HR Staff /Compliance and Audit Staff within the purview of their functions as approved by Chief Risk Officer and Compliance/ Audit Personnel. Persons outside this category requiring access shall obtain clearance from the DH Operations & Business Support.

1. **Customer Accounts**:

Classified as Confidential; Operations, Sales, Compliance, Support and Audit staff shall have access to all customer accounts. Persons outside this category requiring access shall obtain clearance from the DH Corporate XXXXing & Operations

Support staff shall have no access to print customer account statements

IT shall ensure an enabled audit trail is in place to monitor unauthorized access to customer account information.

1. **Office Accounts:**

Classified as Private; Operations and Compliance/Audit staff shall have access to all office accounts. Access to Sales and Support staff will be limited to office accounts within their branch/areas of responsibility. Persons outside this category requiring access shall obtain clearance from the DH Corporate XXXXing & Operations

1. **Staff Information:**

Classified as Private; Access should be limited to Individual staff and their supervisors. Staff of Employee Relations in HR shall have access to all staff information available on Infoshare. Persons outside this category requiring access shall obtain clearance from the Divisional Head Human Resources.

1. **Card Holder Data:**

Classified as Sensitive/Confidential; IT & Digital Compliance, E-Channels and Audit staff shall have access to this information based on business need. Persons outside this category requiring access will not be granted except there is approval from management based on business need.

All appearance of PAN (whether in hard copy or electronic form) must be masked except where there is business justification for it to appear otherwise.

1. **Reports**

Reports available on Infoshare will be made available to persons that requested the report as well as other groups of persons specified to avail the report to.

Subsequent information made available on Infoshare shall follow the classification above.

**2.1.5 Responsibilities**

* All users are required to understand this policy. Any employee found to have violated this policy shall be subject to disciplinary action.
* Access to information classified as Confidential or Private will be authorized by the information owner or any other persons delegated with that authority.
* Head, Information Security & Head, IT & Digital Compliance is responsible for enforcing this policy.
* Internal Audit – IS Audit is responsible for auditing this policy.

**Roles and Responsibility Matrix**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Information Security** | **Information Security Steering Committee** | **IS Audit** | **Users** |
| Ensuring policy is fit for purpose | R/C | A | R | I |
| Annual policy review | R/C | A | I | I |
| Following the policy | R | A | R | R |
| Communication of policy | R | A | I | I |

### Physical Asset and Control Policy

**2.2.1 Overview**

This policy is to ensure that the XXXX take measures to protect its physical assets & resources. This policy will reduce the risk of unauthorized access, loss of, and damage to information during and outside of normal business hours or when physical assets are left unattended.

* + 1. **Purpose**

To establish guidelines and procedures for managing access and classification of XXXX information assets.

**2.2.3 Objectives**

The objective of this document is:

* To improve the security and confidentiality of information
* To ensure that the XXXX’s information and information facilities are well protected

**2.2.4 Policy Details**

* All physical assets shall be classified based on their value and importance. The classification will help determine the necessary controls to implement.
* Classification labels (physical or electronic) shall be given to physical assets to reflect the classification based on the criticality of information they produce and on their use.
* A criticality rating of systems into Critical, Important or Low will be carried out, according to whether the highest rating of the information confidentiality, integrity or availability is high, medium or low respectively. The degree of protection to be accorded each system will be determined by its criticality rating; this rating will be carried out by business owners in conjunction with IT.

1. **Critical** (description of physical asset classified as critical)
2. **Important** (description of physical asset classified as important)
3. **Low** (description of physical asset classified as low)

* All critical physical assets shall have a nominated owner or custodian.
* Information Custodians for all critical physical assets shall be identified. The Information Custodians shall be assigned the responsibility for maintaining appropriate controls over these assets.
* Inventories of all physical assets associated with information provision shall be maintained.
* A detailed inventory listing of all physical assets shall be documented and maintained. Documentation should include:
* Information Custodian: Every critical physical asset shall be assigned an appropriate Information Custodian who is responsible for the information asset
* Identification: Every critical physical asset shall be uniquely identified. The identification scheme used for this must ensure that:
  + The location of the information asset is known
  + The supplier of the information asset is known (supplier information must be available)
  + Maintenance contract(s) for the information assets are identified.
* Description: a short description should be available for every information asset. The description should include general information on the information assets, such as its main function and use.
* Configuration: Technical configuration documentation should be included and supported by business requirements explaining why the physical asset has been configured as such. This documentation should include licensing information.
* Physical assets include manuals, software (applications, tools, and utilities) CDs, equipment and media.
* A formal process shall be in place to capture critical physical assets on the inventory register when purchased, deleted, sold or taken out of use.
* Departing employee must return all information assets and equipment belonging to the XXXX, unless agreed otherwise with the designated owner responsible for the information asset.
* Information Custodians shall be educated on their responsibilities for ensuring adequate protection of their assets; they are ultimately responsible for their assets, but may allocate routine administrative and security responsibilities to a designate.
  + 1. **Responsibilities**
* All users are required to understand this policy and put into action.
* Head, IT is responsible for enforcing this policy.
* Head, Information Security is expected to ensure adherence to this policy
* Internal Audit – IS Audit is responsible for auditing the implementation of this policy.

Violations of the physical asset & control policy will be documented and can lead to revocation of system privileges and/or disciplinary action up to and including termination.

**Roles and Responsibility Matrix**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Information Security** | **Information Security Steering Committee** | **All Users** | **IT** |
| Ensuring policy is  fit for purpose | R/C | A | I | R |
| Annual policy review | R/C | A | I | I |
| Following the  policy | R | A | R | R |
| Communication of policy | R | A | I | R |

### Asset Inventory Policy

**2.3.1 Overview**

Asset inventory involves gathering detailed information which is used to make decisions about information assets purchases and redistribution. It helps organizations manage their systems more effectively and saves time and money by avoiding unnecessary asset purchases and promoting the harvesting of existing resources.

**2.3.2 Purpose**

To establish guidelines and procedures for managing asset inventory

**2.3.3 Objectives**

The objective of this policy is to:

* Track and report the state of the XXXX’s information assets on a routine basis
* Provide specific guidance for calculating and reporting on the total cost of the XXXX’s information assets throughout the asset life cycle
* Leverage the XXXX’s purchasing power by knowing the XXXX-wide need, and the volume and timing of need for future IT hardware and software purchases
* Ensure software license optimization and compliance
* Establish an initial, current and disposal value for the XXXX’s Information assets
* Plan for a common, shared, XXXX-wide information technology infrastructure; and
* Acquire the information needed for XXXX-wide information resources management decision-making
  + 1. **Policy Details**
* A formal Hardware and Software Inventory of all equipment shall be maintained and kept up to date at all times. Where the technology exists, systems / fixed assets XXXX wide shall be managed using an inventory management solution for effective monitoring and depreciation of IT assets.
* Hardware devices shall be named in accordance with the IT Device Naming Convention specified in the IT policy
* Theft/ loss / damage of all physical system assets shall be communicated by custodian / relevant department to the General Service department accordingly within 48 hours.
* All XXXX owned devices must be properly labelled. The label should carry the serial number and tag number of the device.
  + 1. **Responsibilities**
* All users are required to understand this policy
* IT support staff & General Services shall be responsible for implementing this policy.
* Head, IT and Head, General Services is expected to ensure adherence to this policy
* Head, Information Security is expected to ensure adherence to this policy
* Internal Audit – IS Audit is responsible for auditing the implementation of this policy.

Violations of the physical asset & control policy will be documented and can lead to revocation of system privileges and/or disciplinary action up to and including termination.

**Roles and Responsibility Matrix**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Information Security** | **Information Security Steering Committee** | **All Users** | **IT/General Services** |
| Ensuring policy is  fit for purpose | R/C | A | I | R |
| Annual policy review | R/C | A | I | I |
| Following the  policy | R | A | R | R |
| Communication of policy | R | A | I | R |

### Data Retention Policy

**2.4.1 Overview**

The XXXX holds a great deal of important information that is crucial to the running of the organisation. While many information systems can be recovered after an incident, the business critical data that resides in electronic and paper form must be suitably protected. This involves considerations into the confidentiality, integrity and availability (CIA) of business critical and potentially sensitive data. This Policy reflects on the important business information and records that are essential to the ongoing, legal and effective functioning of XXXX. These are distinguished from those documents whose continued preservation serves no useful purpose to the XXXX (e.g. personal e-mails and correspondence, preliminary drafts of documents after the final version has been produced, and unsolicited newsletters and brochures from vendors).

**2.4.2 Purpose**

The purpose of this Data Retention Policy is to provide a legal and business framework for the management, retention, and destruction of XXXX Records. This Policy specifies the retention period during which Records must be retained and after which Records must be destroyed.

This policy is designed to:

* Ensure compliance with all applicable federal and state legal requirements as well as PCIDSS requirements
* Eliminate accidental or innocent destruction of records
* Permit XXXX to identify valuable documents on short notice when needed.

**2.4.3 Objectives**

The objective of this document is to provide guidance on the retention of the various types of data the XXXX holds. This document strives to balance the need to store information with legal obligations to destroy the data safely when it is no longer required.

**2.4.4 Policy Details**

* Unless otherwise specified in this Policy, the following applies to all corporate functions.
* It is the policy of XXXX to preserve all Records for the period of their immediate or current use, unless a longer retention period is necessary for historical reference or to comply with contractual or legal requirements.
* To provide for consistent retention and disposal of common XXXX Records, **Exhibit A- Retention Schedule** is provided in this Policy document and defines a retention schedule that meets XXXX’s business, legal, fiscal, and reference requirements
* Records that serve no useful purpose should be promptly and systematically deleted and destroyed, with the exception of documents that are relevant to or discoverable in pending or potential litigation and other legal and official proceedings.
* Electronic files and documents will be retained as if they were paper documents. Any electronic files which fall into one of the document categories listed in Exhibit A will be maintained for the appropriate period of time
* XXXX employees, officers, and directors shall not knowingly alter, conceal, or destroy a Record with the intent to impede, obstruct or influence an investigation or proper administration of any matter within the jurisdiction of any department or agency of the Federal Republic of Nigeria or in relation to or contemplation of any such matter or case**.**
* Unless specified otherwise in this Policy, the retention period for a Record begins on the date that the Record was received or created by XXXX**.**
* The retention period for Records related to a Court hearing or a compliance violation investigation begins upon the end date of the hearing or compliance violation investigation**.**
* Immediately upon learning of an investigation or court proceeding involving a particular XXXX matter or subject, XXXX (Legal Services) shall notify all employees to preserve all Records pertaining to that matter or subject and to cease and avoid any destruction of the Records pertaining to that matter or subject that would otherwise be authorized by this record retention and destruction policy. In such a case, the retention period for such Records will be specified by the XXXX Legal department.
* Records whose retention period is explicitly stated within this policy, or have a retention period defined by the XXXX Legal department per section 16.2.7 above, must be destroyed within six (6) months of the end date of the Record’s retention period. Records whose retention period is not explicitly defined and is subject to interpretation of immediate or current use must be destroyed within a period of six (6) months from the end date of its immediate or current use, or two (2) years after the Record was created or received. Upon identifying Records whose immediate or current use exceeds two (2) years which are not explicitly defined in this policy, XXXX should consider adding such Records retention period to this Policy.

**Compliance Policy**

This section contains policy specific to compliance program activities.

* All Records generated or received pursuant to the compliance program activities delegated to XXXX, including but not limited to all compliance programs and hearing process activities, shall be maintained for a minimum of ten (10) years, unless a different **retention period is** specified by a CBN or other applicable law.
* For Records received or created as part of compliance program activities, the retention period begins upon the initiation of the compliance program activity that produced the Record, unless the Record is material to the resolution of a controversy or is related to a hearing or compliance violation investigation.
* **T**he retention period for Records material to the resolution of a controversy related to a Court process begins after the controversy is resolved.

**Registered Functions**

This section contains policy specific to XXXX Registered Entity program

* All Records generated or received pursuant to XXXX Registered Entity program activities shall be maintained in accordance with the Corporate Policy, unless identified in Exhibit A below.
* These records include authentication data like PIN Offset stored on PostCard for Online PIN Verification and this will be destroyed securely according to the methods stated in Disposal Policy Section(PCIDSS) when the need arises.
* Card Authentication Values such as; Card Verification Code(CVC), Card Verification Value (CVV, CVV2 etc.) are not stored on any System and therefore are not affected by this Policy(PCIDSS)

**Exhibit A – Retention Schedule**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Record Type** | **1 year** | **2 years** | **3 years** | **7 years** | **Permanent** |
| Accounts payable ledgers & schedules |  |  |  | **Y** |  |
| Accounts receivable ledgers & schedules |  |  |  | **Y** |  |
| XXXX policy and practice manuals |  |  |  |  | **Y** |
| Audit reports |  |  |  |  | **Y** |
| XXXX statements |  |  |  | **Y** |  |
| XXXX reconciliations |  |  |  | **Y** |  |
| Canceled checks |  |  |  | **Y** |  |
| Chart of accounts |  |  |  |  | **Y** |
| Contracts & leases: |  |  |  |  |  |
| * Current |  |  |  |  | **Y** |
| * Expired |  |  |  | **Y** |  |
| Corporate records: |  |  |  |  |  |
| * Board and Committee Meeting Agendas and Minutes |  |  |  |  | **Y** |
| * Subcommittee, Work Group, and Task Force Agendas and Minutes |  |  |  | **Y** |  |
| * Charters |  |  |  |  | **Y** |
| * Bylaws |  |  |  |  | **Y** |
| * Articles of Incorporation |  |  |  |  | **Y** |
| * Annual Reports |  |  |  |  | **Y** |
| Correspondence: |  |  |  |  |  |
| * Contributions |  |  |  | **Y** |  |
| * General |  |  |  | **Y** |  |
| * Legal & important matters only |  |  |  |  | **Y** |
| Routine vendor | **Y** |  |  |  |  |
| Depreciation schedules |  |  |  |  | **Y** |
| Election records |  |  |  |  | **Y** |
| Employee personnel records  (after termination) |  |  |  | **Y** |  |
| Employee payroll tax returns |  |  |  | **Y** |  |
| Employment applications |  | **Y** |  |  |  |
| Financial records/schedules used in preparation of tax returns (from date return filed) |  |  |  |  | **Y** |
| Financial statements (year-end; other months optional) |  |  |  |  | **Y** |
| General ledgers: year-end trial balances |  |  |  | **Y** |  |
| Insurance policies (including expired policies |  |  |  |  | **Y** |
| Inventories |  |  |  | **Y** |  |
| Invoices: |  |  |  |  |  |
| * From vendors |  |  |  | **Y** |  |
| * To customers |  |  |  | **Y** |  |
| Ownership of property, real estate, patents, trademarks, copyrighted documents (from date ownership ends) |  |  |  | **Y** |  |
| Payroll records & summaries |  |  |  | **Y** |  |
| Pension documents & records |  |  |  |  | **Y** |
| Petty cash vouchers |  |  |  | **Y** |  |
| Purchase orders |  |  |  | **Y** |  |
| Receipt records (sales, etc.) |  |  |  | **Y** |  |
| Sales records and journals |  |  |  | **Y** |  |
| Subsidiary ledgers |  |  |  | **Y** |  |
| Tax returns |  |  |  |  | **Y** |
| Vouchers for payments to employees for reimbursements, allowances, etc. |  |  |  | **Y** |  |
| ATM footages and Journal |  |  |  | **Y** |  |
| Customer record |  |  |  |  |  |
| Active/ Dormant Account |  |  |  |  | **Y** |
| Closed Account | **Y** |  |  |  |  |
| ATM Footages |  |  |  | **Y** |  |
| ATM Journal |  |  |  | **Y** |  |
| Card Holder Information (PAN,  Expiry Date etc.) |  |  |  | **Y** |  |
| Camera Data | At least 90 days |  |  |  |  |
| Instant Message | 90 days |  |  |  |  |

### Information Disposal Policy

**2.5.1 Overview**

Confidential electronic and paper information must be disposed of securely to minimize the risk of unwanted disclosure. The XXXX holds and processes a large amount of information and is required to protect that information in line with relevant legislation and in conformity with the XXXX regulations and policies such as the Information Security Policy and the Data Retention Policy. This policy sets out the requirements for staff on the secure disposal of the XXXX’s information

**2.5.2 Purpose**

To establish guidelines and procedures for information Disposal

**2.5.3 Objectives**

The objective of this policy is:

* To ensure that information that is no longer required is disposed in an appropriate manner
* To provide clear guidance on the disposal of specific and general categories of information

**2.5.4 Policy Details**

* The information on any computer hard drive, cell phone, or other electronic device must be erased and not recoverable before the equipment is reassigned within a unit. This information includes (but not limited to) Card Holder Information (PCIDSS) (Consult with IT for further information.)
* All computer systems, electronic devices and electronic media must be properly cleaned of sensitive data and software before being transferred outside of the XXXX either as surplus property or as trash.
* Outdated or broken computer equipment or other electronic devices cannot be discarded in dumpsters or regular trash containers.
* Computer hard drives must be sanitized by using software that is compliant with XXXX standards. Non-rewritable media, such as CDs or non-usable hard drives, must be physically destroyed.

The primary responsibility for sanitizing computer systems, electronic devices and media rests with the units that purchase them.

**Paper records Disposal Policy**

The following methods will be used for Paper Records’ disposal:

* Shredding

The security provided by the shredding of records depends on how fine the paper is shredded. Cross shredding in a two axis shredder may be needed for particularly sensitive documents. Shredded paper may be pulped and recycled, or then used for other purposes such as insulation.

* Pulping

Pulped paper is reduced to its constituent fibres. If carried out correctly, it is a very secure method of destruction. Pulped paper is usually recycled.

* Burning

Burning records is not recommended and should only be used as a last resort if there is no environmentally friendly method of destruction available. Records should be burned in accordance with any environmental guidelines and local burning restrictions. Densely packed paper does not burn well, so burning should be undertaken in an industrial facility (not in a backyard incinerator).

* Any disposal of computer systems and media must comply with all environmental regulations.

**Statement of Policy/Procedure for Destroying Card Holder Information (PCIDSS)**

The retention Periods for Card Holder Information on Postilion Real Time and Postilion Office are defined as follows:

* **Postilion Real Time**: 1 Month (after one month, the data are archived to Postilion Office)
* **Postilion Office:** As defined in Data Retention Policy Section 2.4.4 – Exhibit A

Once the maximum retention period allotted for cardholder data as defined in Section 2.4.4 – Exhibit A is reached, it must be removed from all electronic media, and any hardcopy edition must be disposed of accordingly. Methods for disposal including the following:

* Purging and deleting cardholder data from all system components. This can be done by utilizing a secure wipe program in accordance with XXXX accepted standards for secure deletion (i.e., degaussing). System components are defined as any network component, server or application included in or connected to the cardholder data environment.
* Destroying (cross-shredding) any cardholder data that is in a hardcopy format.

For electronic media stored on system components that are no longer in use, these system components must have cardholder data disposed of via any one of the following procedures:

* Disintegration
* Shredding (disk grinding device)
* Incineration by a licensed incinerator
* Pulverization

All Card Holder information, electronic and hard copy must be destroyed in a timely manner according to the timeframe outlined in Section 2.4.4 – Exhibit A of the Data Retention Policy.

* + 1. **Responsibilities**
* All XXXX employees are responsible for the sanitation of non-reusable electronic media before disposal. Similar to shredding paper reports, CDs and other non-rewritable media should either be broken or defaced by scratching before disposal.
* Heads of Department are responsible for the sanitation of all XXXX owned electronic devices and computer systems in their units prior to removal from the XXXX premises. This responsibility may be delegated within the XXXX as deemed appropriate.
* General Services is responsible for the disposition of surplus computer systems and electronic devices. Any computer system or device sent to General Services for disposition must have an Electronic Data Disposal Verification form (available from IT) affixed to it indicating that the system has been sanitized, the date, the name and phone number of the person responsible for sanitizing the system. General Services will not accept any computer system without this information.

**Roles and Responsibility Matrix**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Information Security** | **Information Security Steering Committee** | **All Users** | **IT/General Services** |
| Ensuring policy is  fit for purpose | R/C | A | I | R |
| Annual policy review | R/C | A | I | I |
| Following the policy | R | A | R | R |
| Communication of policy | R | A | I | R |

1. **System Documentation Policy**

**2.6.1 Overview**

Good system documentation enhances and validates security by documenting the configuration details and procedures that support a security policy. System documentation also serves as an important part of backup and disaster recovery documentation. Good documentation must be thorough and must be kept current.

**2.6.2 Purpose**

To establish guidelines and procedures for managing system documentation

**2.6.3 Objectives**

The objective of this policy is:

* To identify systems that need improvement.
* To provide system details that are necessary in planning upgrades
  + 1. **Policy Details**
* All the XXXX’s information systems shall have adequate systems documentation
* System documentation shall reside with the custodian of the respective application in IT and must be securely stored at all times
* Version updates to system documentation shall be appropriately maintained, stored and provided to system users / support staff on a need basis
  + 1. **Responsibilities**
* IT support staff & General Services shall be responsible for implementing this policy.
* Head, IT and Head, General Services is expected to ensure adherence to this policy
* Internal Audit – IS Audit is responsible for auditing the implementation of this policy.

### Acceptable Use Policy

**2.7.1 Introduction**

Information Assets are strategic assets of the XXXX and must be treated and managed as valuable resources. The XXXX provides various information assets to be used for business purposes in serving the interests of the XXXX, and of our clients and customers in the course of normal operations. This Acceptable Use Policy (AUP) is designed to protect XXXX., our employees, customers and other partners from harm caused by the misuse of our information and information assets. As such, all employees and users must ensure they adhere to the guidelines in this policy at all times. Managers are responsible for ensuring all people working for XXXX in any capacity receive a copy of these policies, read them and understand them. All users must manage them responsibly to maintain the confidentiality, integrity, and availability of the XXXX’s information assets.

**2.7.2 Purpose**

This Policy is established to achieve the following:

* To establish appropriate and acceptable practices regarding the use of the XXXX’s information assets.
* To ensure compliance with applicable policies regarding the management of information resources.
* To educate individuals who may use information assets with respect to their responsibilities.

**2.7.3 Objectives**

The objective of this document is to protect the confidentiality and integrity of information and privacy of its customers and users.

**2.7.4 Policy Details**

**General Summary**

1. Users shall ensure that the XXXX’s information assets are used appropriately for approved business purposes. Employees shall exercise good judgment regarding appropriate use of the XXXX's information assets.
2. The management reserves the right to monitor the information stored on any device belonging to the XXXX.
3. Users are responsible for the protection of information in their custody or stored/processed on computing systems.
4. The user of the XXXX’s information systems and communication resources is a revocable privilege; the XXXX reserves the right to disconnect any device that interferes with the XXXX’s network.

**Monitoring**

* The XXXX reserves the right to monitor usage patterns of its e-mail and internet communications, equipment and telephone logs for the purpose of maintaining, investigating or detecting abuse, detecting spam, viruses and attachments and other security issues
* The XXXX reserves the right to access and monitor all information, messages and files on its information systems, e-mail or internet system.
* The XXXX may implement tools that block usage and access to internet for productivity or security reasons
* The XXXX reserves the right to audit systems to ensure compliance with this policy

**Appropriate Use**

* Information assets are provided for business use only. Any use of equipment for personal use is strictly limited.
* When at social gatherings or while using social media, users shall not disclose sensitive information or discuss business details.
* Users are prohibited from conducting any activities which may be deemed as inappropriate or offensive to the XXXX’s users and customers.
* Users should not view, store, copy or transmit inappropriate and unlawful content using the XXXX’s resources.
* Data theft in any form or use of unauthorized storage devices is strictly prohibited.
* Users are not permitted to use e-mail, the internet, telephone, Information or other systems for personal or commercial purposes
* Users must be aware that all materials (electronic or otherwise) created by you or amended by you in the course of your duties while you are working for, or on behalf, of XXXX belongs to the XXXX

**Working Securely**

* Users shall ensure that no one uses their login ID (including your colleague or manager) or use another person’s login ID to access any systems or send e-mails
* Do not write down your password. If you believe someone else knows your password change it immediately. Do not give your password to anyone else, including service desk staff.
* When creating passwords do not use words in dictionaries, but where possible use a combination of letters, numbers, upper and lower case and/or punctuation characters.
* Do not have your terminal, computers and laptops unattended without locking the screen or logging out.
* Do not ever attempt to circumvent or defeat security or audit controls unless specifically authorised to do so by IT & Digital Compliance/Information Security Team.
* Do not reply to unsolicited e-mails (Spam). Contact the Information Security team if you suspect a mail to be Spam.

**Appropriate use of software, equipment and information**

* Users shall ensure all software to be used has been approved by IT/Information Security in advance, correctly licensed, installed by authorised staff and used in accordance with licensing agreements.
* Users shall not install, link or attach any equipment to the infrastructure unless this has been specifically approved by IT via its Change management process.
* You may only access, copy, amend or delete any information that you are authorised to use.
* Inserting or attaching any removable device to any system is prohibited. If required, user shall get approval from the information security team to do so and such devices must not contain viruses or other malicious programs. If uncertain, ask IT or IT service desk to check the device.
* Users shall not make illegal or unauthorized copies of any the XXXX’s proprietary and copyrighted material. This includes, but is not limited to, text, graphics, photos, videos, music, clipart, source code, files, and so on.

**Potential Loss of data**

* Inform IT and IT Service desk of any theft or loss of any piece or equipment or data e.g. Laptops, mobile devices (Tablets, phones) or other storage media containing the XXXX’s data.

**System or Data Access**

* Inform IT Service desk/ Information Security if you need any change in access to any of the XXXX’s information systems. HCM will inform IT when you leave or change roles. This ensures you can be given the required system access.
* Inform Information Security if you suspect someone of trying to access data for which they do not have authorization

**Documents and Print Outs**

* Users are required to classify and handle documents as defined in the Information Classification and Control Policy
* Un-used documents/papers to be destroyed securely by using shredder machines.
* Users to adopt a clean desk policy for papers in order to reduce the risk of unauthorized access and misuse.
* Users are required to lock sensitive documents under lock and key before leaving office.

**Appropriate use of E-mail and Internet**

* Alternate messaging systems such as instant messaging, public email or chats e.g. Hotmail, Yahoo, Gmail etc.), to conduct the XXXX’s business is prohibited.
* Users should avoid sending unsolicited e-mail messages, including send "junk mail", “e-mail spam” or other advertising material to individuals who did not request such material.
* Users are required to use extreme caution when opening e-mails or attachments which appear dubious or suspicious in any way. If you are warned of or suspect a computer virus infection, hoax or persistent spam, kindly report it to the IT service desk.
* Users should be aware that the content of e-mails is not private. Any comments made about an individual in an e-mail may be disclosed to them in the course of an investigation.
* No user shall use the XXXX’s information systems in any way that may be interpreted as insulting, disruptive or offensive by any other person, which may be harmful to the company’s reputation. This includes forwarding any received e-mail. Examples of prohibited materials include:
  + Sexually explicit messages, images, cartoons, or jokes
  + Unwelcome propositions, requests for dates, or love letters
  + Profanity, obscenity, slander, or libel
  + Ethnic, religious, or racial slurs
  + Political beliefs or commentary
  + Any other message that could be construed as harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin, disability, or religious or political beliefs
* Users should avoid using the XXXX’s confidential information when they are accessing the internet
* Users shall not view or download any pornographic, obscene or offensive material
* Users shall not download files from external sources, including bulletin boards unless approved by IT. The risk is that viruses could be imported.
  + 1. **Responsibilities**
* All users are required to understand and comply with this policy at all times.
* Managers are responsible for ensuring all users in their units in any capacity receive a copy of these policies, read them and understand them.
* Head, IT is responsible for implementing this policy
* CISO and Head ISM are responsible for ensuring adherence to this policy
* Internal Audit – IS Audit is responsible for auditing the implementation of this policy.

**Roles and Responsibility Matrix**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Information Security** | **Information Security Steering Committee** | **IT** | **All Users** | **Managers** |
| Ensuring policy is  fit for purpose | R/C | A | R | I | I |
| Annual policy review | R/C | A | C | I | I |
| Following the  policy | R | A | R | R | R |
| Communication of policy | R | A | R | I | R |

### Access Control Policy

**2.8.1 Introduction**

Access to information and information systems is a fundamental aspect of Information Security. Access control is concerned with determining the allowed activities of legitimate users, mediating every attempt by a user to access a resource in the system. The access control policy provides the guidance on access control to information systems and applications, either allowing or restricting authorization of information systems. This allows for the preservation of confidentiality within the XXXX and protects the XXXX’s information and information systems from unauthorized access.

**2.8.2 Purpose**

The purpose of this policy is to establish directives, which will forestall uncontrolled or unauthorized access, misuse of user privileges, or unauthorized disclosure to third parties, that may result in security breaches, malicious damage, misuse, or theft of corporate resources.

**2.8.3 Objectives**

The objectives of this document are:

* To ensure that business, legal and security requirements drive the authorization process and access to information and information assets.
* To limit access to information and information processing facilities.
* To ensure authorized user access and to prevent unauthorized access to systems, applications and services

**2.8.4 Policy Details**

* Access to information and information assets must be commensurate with the security requirements of that resource and the classification of data it provides access to.
* Access to all information and information systems XXXX wide shall be granted to all users based on the principle of least - privilege

**User Registration and De-registration**

* All new employees shall attend the mandatory information security awareness training as part of induction before being granted access to the XXXX’s network and information systems.
* All new employees shall be required to read and sign the acceptable usage policy prior to being granted access.
* On the resumption of all new employees, access to the XXXX’s network and systems shall begin with a formal notification from Human Capital management Unit to the Information Technology Unit.
* By default, all configured employees shall have access to receive emails and send emails either via Microsoft Outlook or Outlook Web Access.
* Based on user’s IT requirements for his/her job function as advised by HCM/Line Manager, IT shall create a user’s profile on the group network while Information Security shall create user accounts on requested business applications.
* All Core XXXXing Applications e.g. Finacle users (especially those handling financial transactions) will be profiled to have Second Factor Authentication (Token) apart from their username and password
* User accounts shall be promptly deactivated whenever employee is on vacation, leave of absence or even suspension.
* User accounts shall be promptly revoked when no longer required, particularly upon staff / contractor disengagement, to forestall unauthorized access to the system.
* To facilitate prompt account deactivation or termination, HCM shall send list of staff on vacation, suspension or disengaged, to IT, Information Security and other responsible units who will then deactivate / delete such user account from the network and system within one working day of receipt of notification.
* All employees leaving the XXXX must return their assigned IT systems and access rights must be revoked prior to leaving the XXXX.

**Privilege Management**

* The principle of least privilege must be applied at all times.
* Allocation of user privileges must be based upon the following criteria: system and data classification, business requirements, job function, related responsibilities or “need to know or use
* The principles of separation of duties must be applied when assigning job responsibilities and roles relating to restricted or IT Resources identified as mission critical and classified as high sensitivity.
* Unique roles and responsibilities must be assigned with consideration for the segregation of access control roles (i.e. access request, access authorization, and access administration) and management to reduce the risk of accidental or deliberate system or application misuse.
* Third-party programmers must not be granted direct access to XXXX’s application source code. Only the modules needed for a specific programming task may be revealed to these programmers. These programmers must additionally never be given privileges to directly update the source or object code.
* All requests for change of user privileges on applications must be sent to Information Security and duly approved by the user’s line managers. This must be supported by a completed and authorised system access form.
* The technique of dual control and segregation of duties shall be employed to enhance the control over procedures whenever both the risk and consequential impact of a related information security incident would likely result in a financial or material damage to the XXXX.
* IT Staff that perform critical functions (Database Administrator, Unix Administrator, System Administrator etc.) shall have separate user account / logons to reduce the risks of unauthorized or unintentional modification or misuse of the XXXX’s assets / data.
* Where segregation of duties cannot be in place, audit logs shall exist and must be reviewed.
* Adherence to the segregation of duties shall be monitored by the IT & Digital Compliance and Internal Audit team.
* All privileges for any user shown to be engaged in abusive or criminal activity must be immediately revoked.
* The Head, IT and Head, IT & Digital Compliance will maintain a master list of privileged accesses, which are in use, and this will be checked and confirmed by the ISO on a quarterly basis. The list will identify all separate logons for each system and application.

**User Password Management**

* All allocation of passwords must be through a formalized and preferably automated process requiring users to change their passwords at periodic intervals and restrict re-use of previously used passwords. Kindly refer to the Password Policy.

**Review of User Access Rights**

* User accounts, privileges, access and authorization in all systems (e.g. Finacle, Active Directory as well as within applications themselves) must be reviewed at regular intervals with the aim of ascertaining and reporting inactive accounts and disabling them.
* Privileges granted to users must be re-evaluated by the user’s immediate manager/HCM to determine whether currently-enabled system privileges are needed to perform the user’s current job duties or not and must inform the Information Security/Information Technology team for further actions.
* Where a user account has been inactive on a system for a period exceeding 30 days, user account/access shall be disabled immediately, and an enquiry shall be raised to verify why access has not been used.
* Where a user account is no longer required by a user, such user account shall be deleted from the system or network.

**User Responsibilities**

* Users are responsible for handling, use and storage of passwords in a manner that complies with all password policy requirements
* Users are responsible for ensuring that unattended equipment has appropriate protection.
* Users are responsible for ensuring that information contained in papers and removable storage media on their desks, as well as information on their computer screens, has appropriate protection and complies with all Clear desk and clear screen policy requirements

**System and Application Access Control**

* Access within software applications must be restricted using the security features built into the individual product. The access must:
* Be compliant with the User Registration/De-registration and privilege management above and the Password policy.
* Be separated into clearly defined roles.
* Give the appropriate level of access required for the role of the user.
* Be unable to be overridden (with the admin settings removed or hidden from the user).
* Be free from alteration by rights inherited from the operating system and utility programs that could allow unauthorised access or privilege.
* Be logged, monitored, and auditable.
* All applications and systems must adopt secure log-on procedures that minimize the opportunity for unauthorized access
* All applications and systems must have procedures in place to shut down inactive sessions after a defined period of inactivity.
  + Window session must have a maximum idle session timeout of five (5) minutes
  + Finacle session must have a maximum idle session timeout of seven (7) minutes
  + Unix Operating System must have a maximum idle session timeout of twenty (20) minutes due to multistep tasks like log review and likely data loss could frustrate users
* Access to system and application source code must be restricted.
  + 1. **Responsibilities**
* All users are required to understand and comply with this policy at all times.
* Head, IT and Head, IT & Digital Compliance are responsible for implementing this policy
* CISO and Head ISM are responsible for ensuring adherence to this policy
* Internal Audit – IS Audit is responsible for auditing the implementation of this policy.

**Roles and Responsibility Matrix**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Information Security** | **Information Security Forum** | **IT** | **IT & Digital Compliance** | **All Users** |
| Ensuring policy is  fit for purpose | R/C | A | R | R | I |
| Annual policy review | R/C | A | C | C | I |
| Following the  policy | R | A | R | R | R |
| Communication of policy | R | A | R | R | I |

### Human Resources Security Policy

**2.9.1 Overview**

Information security is very important to help protect the interests and confidentiality of the XXXX and its customers. Information security cannot be achieved by technical means alone. Information security must also be enforced and applied by people, and this policy addresses security issues related to employees of XXXX.

**2.9.2 Purpose**

The purpose of this policy is to set out the processes and responsibilities that are necessary to ensure that the employees of XXXX contribute to the security of its information and information assets.

**2.9.3 Objectives**

The objective of this policy is:

* Ensure that all users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of the XXXX’s information facilities
* To maintain the security of the XXXX’s information and information systems that are accessed, processed, communicated to, or managed by third parties
* To ensure that all users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support XXXX security policy in the course of their normal work, and to reduce the risk of human error.
* To ensure users exit the XXXX or change employment in a secured manner.

**2.9.4 Policy Details**

Human resources security responsibilities shall be addressed prior to employment, during employment, change of employment and termination and this will be included in contracts and monitored during an individual's employment. In order to fulfil this policy, the following statements shall be adhered to:

* All employees must comply with the information security policies of the XXXX. Any information security incidents resulting from non-compliance will be documented and can lead to revocation of system privileges and/or disciplinary action up to and including termination.
* Human Capital Management recruitment verification checks on new employee shall be performed.
* The terms and conditions of employment shall include requirements for compliance with information security policies.
* A written undertaking shall be obtained from agencies (outsourced parties) providing temporary employees that appropriate character and business references have been obtained for such employees
* Indemnity Clauses relating to restitution to XXXX in instances of negligence by employee from agencies (outsourced parties) shall be included in contracts.
* All external suppliers who are contracted to supply services to the XXXX must agree to follow the information security policies of the XXXX.
* Non-disclosure agreements must be used in all situations where the confidentiality, sensitivity or value of the information being disclosed is important.
* Contractors shall not be allowed in sensitive areas (e.g. computer rooms), without supervision and authorisation.
* All new employees shall attend the mandatory information security awareness training as part of induction before being granted access to the network or systems. Where employee change jobs, their information security needs must be reassessed and any new training provided as a priority.
* Before a leaver is issued with a clearance letter, CISO shall issue clearance to HCM reflecting that all information assets of the officer have been properly retrieved and assigned access rights have been removed.
* Temporary employee shall not be granted access to the network or authorised to use any systems except office productivity tools without the approval of the CISO.
* Employee’s compliance with information security policies shall be monitored.
* Management shall ensure that policies are complied with through regular review and monitoring.
* Segregation of duties shall be implemented ensuring that posting and authorising transactions on critical systems are carried out by separate individuals.
* An employee resigning from XXXX shall send a copy of his/her resignation to Human Capital Management who shall notify Information Technology.
* Departing employee must return all information assets and equipment belonging to the XXXX, unless agreed otherwise with the designated owner responsible for the information asset.
* XXXX shall not recruit spouses or siblings.
* End-users shall be fully trained in the correct use of IT facilities including logon procedures, use of software packages, etc. before they are given access to the IT facilities, to reduce the likelihood of errors.
* Managers shall monitor the work performance of their employee and hold periodic appraisals to identify training needs and to discover any problem areas, particularly where employee deal with sensitive information or work on sensitive computer applications.
* Employees shall receive training in emergency procedures, first aid treatment and the use of fire fighting and other emergency equipment.
* All employees shall be educated on business continuity.
* The disciplinary process for employees shall include sanctions (which may include dismissal) for employee who violates XXXX’s information security policies and procedures. This will be developed by the CISO in collaboration with HCM and approved by the board.

**2.9.5 Responsibilities**

* All users are required to understand this policy and put into action.
* Head, Human Capital Management is responsible for implementing this policy.
* Head, Information Security is expected to ensure adherence to this policy
* Internal Audit – IS Audit is responsible for auditing the implementation of this policy.

**Roles and Responsibility Matrix**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Information Security** | **Information Security Forum** | **All Users** | **HCM** |
| Ensuring policy is  fit for purpose | R/C | A | I | R |
| Annual policy review | R/C | A | I | I |
| Following the  policy | R | A | R | R |
| Communication of policy | R | A | I | R |

### Password Policy

**2.10.1 Overview**

Passwords are an important aspect of information security. A password is a secret word or string of characters that is used for authentication purposes. They are necessary to ensure personal security, to protect the XXXX’s information assets and satisfy information security standards. A poorly chosen password may result in unauthorized access and/or exploitation of the XXXX’s resources. All users, including contractors and vendors with access to XXXX systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

**2.10.2 Purpose**

To establish guidelines and procedures for secure creation and management of passwords in ways that maximizes information security within the XXXX’s network.

* + 1. **Objectives**

The objective of this document is to ensure that the allocation, regulation and change of password rules of and within the XXXX is effectively coordinated

**2.10.4 Policy Details**

**Password Standards**

* Every user with access to the XXXX’s network must have a unique username assigned only to his/her account. In the same vein, access to systems in the XXXX shall only be granted to unique usernames, group usernames shall not be permitted.
* Passwords should neither be too short nor too long. The length of the password will, at all times, comply with the laid down password creation rules. A passphrase can be used when available at application level.
* Password
* All user-level and system-level passwords must conform to the password complexity guidelines.
* Passwords must not be inserted into email messages or other forms of electronic communication
* Passwords are case sensitive and must be used in the exact case they were created**.**
* All vendor-supplied default passwords (including SNMP community strings) must be changed before any computer or communications system is used. These passwords must comply with the requirements set out in this policy – complexity, length, age, etc.
* The sharing of passwords is strictly prohibited in the XXXX. The act of a user login on for another in order to take advantage of his/her privileges is also considered as password sharing
* User shall have access to change his/her password at any time with the system. If a user requires his/her Network Active Directory password to be reset by the system administrator without being physically present, the user’s line manager or HCM is to verify the user’s identity by sending an email for this purpose
* Whenever there is a suspected password compromise, the affected user must change his/her password immediately and report to IT Service Desk for appropriate action.
* Where access is provided to XXXX Networks via remote access mechanisms, this shall be controlled using either a one-time password or a public/private key system with a strong passphrase.
* All passwords for system level accounts, application administrative accounts, system administrator accounts, and database administrator accounts, key business applications must have the following characteristics:
* Must be changed at least once every 60 days.
* Initial password must be changed by logging into the system within 10 days of issue.
* Network passwords for end users shall be changed every 30 days
* Network Password for end users shall be set to NOT EXPIRED upon the following:
* There must be a request to IT through CISO
* Instances: Leave of Absence, Leave above 30days
* Staff Category: Assistant General Manager (AGM) and above
* Request Approval: CISO
* Request Awareness: CCO

**Password Complexity Guidelines**

* All passwords must be at least eight characters long
* All passwords must be alphanumeric i.e. contain letters and numbers
* All passwords should have a combination of upper- and lower-case characters (Capital and Small letters)
* All passwords must include special characters such as (!, \*, #, @, &, %, $)
* Passwords or parts of the password cannot be re-used when creating new passwords
* Passwords should not be particularly identifiable with the user (such as first name, last name, spouse name, pet’s name etc.)
* Passwords must not contain common words or words found in any dictionary
* The password must not contain the user’s login name

**Password Protection**

* Initial Passwords shall be communicated to the user securely
* At no time shall a user on the XXXX domain provide his/her login credentials or email password to anyone, not even family members
* Employees, Vendors and Contractors must not share passwords with anyone. All passwords are to be treated as sensitive, confidential information
* Employees, Vendors and Contractors must not write passwords down and store them anywhere in the office. Passwords are not to be stored in a file on any computer system without encryption.
* If an account or password is suspected to have been compromised, report the incident to security administrator and change all passwords
* Passwords must not be revealed over the phone to anyone.
* Do not reveal a password on questionnaires or security forms
* Password cracking may be performed on a periodic or random basis by the security administrator. If a password is guessed or cracked during one of these scans, the user will be required to change.

**Application Development**

Applications to be deployed in the XXXX must follow the following standard:

* Applications should support authentication of individual users, not groups
* Applications must be configured to force password change upon first login
* Applications should not store passwords in clear text or in any easily reversible form.
* Applications should conform to password complexity guidelines as stated above.
* Applications should provide for some sort of role management; such that one user can take over the functions of another without having to know the other's password.
* Applications should enforce regular password changes and not permit previous password(s) to be reused for at least six usages after being changed
* Applications should support TACACS+, RADIUS and/or X.509 with LDAP security retrieval wherever possible.
* Applications should mask, suppress, or otherwise obscure passwords as entered by users so that unauthorized parties will not be able to observe or subsequently recover them.

**2.10.5 Responsibilities**

* All users are required to understand this policy and put into action. Users are responsible for selecting and securing their passwords.
* Head, IT & Head, IT & Digital Compliance is responsible for implementing this policy.
* Head, Information Security is expected to ensure adherence to this policy
* Internal Audit – IS Audit is responsible for auditing the implementation of this policy.

**Roles and Responsibility Matrix**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Information Security** | **Information Security Steering Committee** | **All Users** | **IT / IT & Digital Compliance** |
| Ensuring policy is  fit for purpose | R/C | A | I | R |
| Annual policy review | R/C | A | I | I |
| Following the  policy | R | A | R | R |
| Communication of policy | R | A | I | I |

1. **E-mail Security Policy**

**2.11.1 Overview**

Electronic mail (e-mail) simply put, is the transmission of computer-based messages – text, images, forms, attachments, data or other communication – over telecommunication channels. E-mail systems are used to send, receive and store messages, including attachments where applicable. At the same time, misuse of email can create legal, privacy and security risks, thus it’s important for users to understand the appropriate use of electronic communications.

**2.11.2 Purpose**

* To establish guidelines and procedures for the proper use of XXXX’s e-mail system and make users aware of what the XXXX considers acceptable and unacceptable uses of the e-mail system
* To establish the criteria governing the authorized use of personal or corporate owned smartphone and tablet (mobile) devices where the owner has established access to the XXXX’s email systems enabling them to send or receive work related email messages and conduct other XXXX business

**2.11.3 Objectives**

The objective of this document is to ensure that:

* The need for secure e-mail usage is communicated effectively
* The XXXX’s email assets and information facilities are adequately used

**2.11.4 Policy Details**

**General**

* All email accounts maintained on the XXXX’s email system are property of the XXXX and are primarily provided for official purposes.
* Extensive use of e-mail privileges for personal purposes is considered a violation to this policy; only limited personal use of the XXXX’s e-mail system is permitted. Personal use of e-mail system must not interfere with normal business activities, must not involve solicitation, must not be associated with any for-profit outside business activities or any potential embarrassment to the XXXX.
* The standard client for e-mail access in the XXXX shall be Microsoft Outlook, Exchange ActiveSync and OWA
* Users who receive confidential information accidentally shall notify the sender and delete such email immediately
* Attachment of data files to email shall only be permitted after confirming the classification of the information being sent and then having scanned and verified the file for the possibility of a virus or other malicious code
* Forwarding or use of Confidential and Confidential documents or emails shall be restricted using Rights Management (RMS) which allows users to decrypt and open right protected messages and documents. RMS will allow publisher of document to set rights management on the document, control usage and distribution of sensitive information by having a reliable enforcement method.
* All users on the XXXX's e-mail platform shall be provided unique e-mail addresses. The e-mail addresses shall be constructed in line with the following naming convention: firstname.surname@XXXX.com However, where there are conflicts (e.g., where two or more staff have similar first and last names) the middle name shall be included to differentiate – firstnamemiddlename.surname@XXXX.com
* Information Technology is responsible for the administration, maintenance and operation of the XXXX’s e-mail system, including the messages stored or transmitted through it. Except by management approval, IT does not have the right to view, delete, or in any other way, modify users’ e-mail messages.
* E-mail accounts are to be used only by the authorized owner of the account name. Account owners shall be held responsible for all activities performed through their account.
* Users accessing their emails from public facilities, e.g. cyber cafes, must exercise due care to ensure that the XXXX’s information is not by any means revealed to unauthorized persons.
* Users must not employ any electronic mail addresses other than official electronic mail addresses for XXXX business messages. Where official electronic mail addresses are unavailable, management approval must be sought before other e-mail addresses can be used for official communication.
* Users must verify/validate the correctness/appropriateness of email addresses to ensure that XXXX’s emails are not sent to unauthorized recipients.
* Broadcast of technical information to all staff shall be permitted for some teams using specialized email accounts as the need arises. However, other staff whose job functions require them to send mails to all staff of the XXXX shall require management approval.

**Prohibited Use**

* Use of e-mail account assigned to another individual to either send or receive messages by a staff. If there is need to read another staff’s e-mail in their absence (while they are away on vacation, for instance), prior approval shall be required for this.
* Forwarding of documents, records and email correspondence deemed confidential and sensitive to third parties outside the XXXX network without the written consent of the Head, Legal Services or designate.
* Unauthorized modification or alteration of email messages. Such modification includes forging and removing information appearing anywhere in an email message including the body of the message or the header (this applies to mail trails also).
* Initiating or forwarding chain mails or spam from any XXXX email account or computer system, or any device used to access the XXXX’s information asset. Any user that discovers spam in the XXXX or associated with the XXXX’s email should report to the IT Service desk immediately for appropriate action.
* Opening of e-mail attachments from unknown or untrusted parties. Such attachments must be deleted immediately or forwarded to IT Service Desk for investigation.
* Transmission of copyrighted materials via the XXXX’s e-mail system without appropriate permission.
* Using the XXXX’s e-mail systems to distribute, disseminate or store indecent, disruptive, discriminatory or harassing materials. Such materials include comments about race, religious and political beliefs, pornography, hoaxes, etc. Employees who receive such email messages from any staff of the XXXX should report to Human Resources immediately.
* Any other use of the e-mail system in a way that violates the requirements of the XXXX’s policies.
* Monitoring of e-mail messages passing through the XXXX’s e-mail system without management approval.
* Forwarding of mails containing the XXXX’s sensitive information outside the XXXX’s network (i.e. to third parties) without management approval
* Sending of anonymous or pseudonymous e-mails to any recipient.

**Monitoring**

* The XXXX is committed to protecting user privacy. However, management reserves the right, employing any preferred means, to monitor, read and keep record of the content of all e-mail transmitted on the network using the e-mail system.
* Electronic mail messages flowing through the XXXX systems may be monitored for internal policy compliance, suspected criminal activity, and other systems management reasons. In the same vain, the content of e-mail messages may be disclosed to law enforcement officials without prior notice to the staff that may have sent or received such messages.

**Retention and Mailbox Limits**

* Information technology shall establish and maintain a systematic process for the recording, retention, and destruction of electronic mail messages for a certain period based on levels. The destruction of the referenced electronic mail messages shall be differed if and whenever any event that may require investigation or legal actions is noticed.
* E-mail quota shall be allotted to users on the XXXX’s e-mail system based on each user level or group/category
* Users shall be responsible for managing the size of their mailbox to remain within the allocated quota. However, rare quota increases shall be granted on a case-by-case basis upon due approval by the requesting user’s group head and the Head, IT; this must be accompanied by appropriate business justifications.
* Default attachment sizes shall be limited to the size of 5MB for users. Attachments containing executable files i.e. files with extensions like .exe, .com, .bat, (including those contained in zipped files) shall be blocked by the email system.

**Mobile Device Email Usage**

* The usage of e-mail on mobile devices must comply with the XXXX’s overall E-mail security policy
* Users using mobile devices to access the XXXX’s e-mail shall be responsible for the protection of the XXXX’s information on these devices
* Users are responsible for ensuring the operating systems on their mobile devices are updated regularly.
* Users are responsible for securing their device to prevent sensitive data from being lost or compromised and to prevent viruses from being spread. – Please refer to the Antivirus Policy
* Devices used to access the XXXX’s e-mail must at a minimum be protected by passwords/passcodes and these passwords /passcodes must have a minimum length of 4 characters.
* Users are prohibited from copying sensitive data from e-mail applications to other applications on the device or to an unregistered personally owned device.
* Devices used to access the XXXX’s e-mail must not be given out (sold, given as gift to non-staff members, etc.) without first notifying the IT Service Desk.
* Users using their mobile devices to access official e-mails must ensure adequate physical protection of the devices at all times; such devices must not be left unsupervised.
* Devices that are lost or stolen, or are believed to have been compromised in some way, must be reported immediately to IT Service Desk so that e-mail access can be deactivated
* The Information Security Unit reserves the right to carry out spot checks of the configuration of devices used to access official e-mail to ensure compliance with the requirements of this policy
* The XXXX reserve the right to block email access, remote-wipe of XXXX content or reset to factory settings on the registered mobile device

**Email Backup, Recovery and Availability**

* Backup tapes created by Information Technology shall solely be for the purpose of restoring the email system in the event of disaster. These tapes may not allow for restoration of individual mailboxes and cannot be used as a convenience to retrieve "deleted" messages.
* Backups do not replace records retention; they are requirements for disaster recovery. Each user must make provisions to retain messages in accordance with applicable XXXX, department, regulatory and legal records retention provision.
* Information Technology shall make all efforts to ensure availability of the e-mail systems; these efforts include providing e-mail processing systems at alternate locations.

**2.11.5 Responsibilities**

* All users are required to understand this policy and put into action.
* Head, IT is responsible for implementing this policy.
* Head, Information Security is expected to ensure adherence to this policy
* Internal Audit – IS Audit is responsible for auditing the implementation of this policy.

**Roles and Responsibility Matrix**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Information Security** | **Information Security Forum** | **All Users** | **IT** |
| Ensuring policy is  fit for purpose | R/C | A | I | R |
| Annual policy review | R/C | A | I | I |
| Following the  policy | R | A | R | R |
| Communication of policy | R | A | I | I |

1. **Internet Usage Policy**

**2.12.1 Overview**

The Internet is a worldwide connection of computer networks that provides unlimited access to communication services and information resources to users worldwide. The internet, by its nature, is borderless, thereby providing unrestricted access to users from different part of the globe. This portends great risks to organization if internet activities are not controlled. In view of the wide use of the internet and the attendant risks, the policies in this document are provided to ensure the safe usage of internet services in XXXX.

**2.12.2 Purpose**

To establish guidelines and procedures for using XXXX’s network to access the internet. These guidelines are designed to ensure that adequate protection is in place for the continuous availability, integrity and confidentiality of the XXXX’s internet services.

**2.12.3 Objectives**

The objective of this document is to ensure that:

* the need and use of the internet is communicated effectively
* the XXXX’s assets and information facilities are adequately protected from misuse of the internet

**2.12.4 Policy Details**

It is the policy of the XXXX that all access to the Internet will be provided to all users to support business activities and only on an as needed basis to perform their jobs and professional roles.

**Resource Usage**

* Access to the Internet will be approved and provided only if reasonable business needs are identified.
* Internet services will be granted based on an employee’s current job responsibilities.
* User Internet access requirements will be reviewed periodically by the IT department to ensure that continuing needs exist.
* Management reserves the right to add or delete services as business needs change or conditions warrant. All other services will be considered unauthorized access to/from the Internet and will not be allowed

**Allowed Usage**

* Internet usage is granted for the sole purpose of supporting business activities necessary to carry out job functions. All users must follow the corporate principles regarding resource usage and exercise good judgment in using the Internet. Questions can be addressed to the IT Helpdesk.
* Acceptable use of the Internet for performing job functions might include:
* Communication between employees and non-employees for business purposes;
* IT technical support downloading software upgrades and patches;
* Review of possible vendor web sites for product information;
* Reference, regulatory or technical information;
* Research

**Personal Usage**

* Using the XXXX’s computer resources to access the Internet for personal purposes, without approval from the user’s manager and the IT department, may be considered cause for disciplinary action up to and including termination.
* All users of the Internet should be aware that the XXXX’s network creates an audit log reflecting request for service, both in-bound and out-bound addresses, and is periodically reviewed.
* Users who choose to store or transmit personal information such as private keys, credit card numbers or certificates or make use of Internet "wallets" do so at their own risk. The XXXX is not responsible for any loss of information, such as information stored in the wallet, or any consequential loss of personal property.

**Prohibited Usage**

* Acquisition, storage, and dissemination of data which is illegal, pornographic, or which negatively depicts race, sex or creed is specifically prohibited.
* The XXXX also prohibits the conduct of a business enterprise, political activity, engaging in any form of intelligence collection from our facilities, engaging in fraudulent activities, or knowingly disseminating false or otherwise libellous materials.
* Other activities that are strictly prohibited include, but are not limited to:
* Accessing the XXXX’s information that is not within the scope of one’s work – this includes unauthorized reading of customer account information, unauthorized access of personnel file information, and accessing information that is not needed for the proper execution of job functions;
* Misusing, disclosing without proper authorization, or altering customer or personnel information;
* This includes making unauthorized changes to a personnel file or sharing electronic customer or personnel data with unauthorized personnel;
* Deliberate pointing or hyper-linking of the XXXX’s web sites to other Internet/WWW sites whose content may be inconsistent with or in violation of the aims or policies of the XXXX;
* Any conduct that would constitute or encourage a criminal offense, lead to civil liability, or otherwise violate any regulations, local, state, national or international laws;
* Use, transmission, duplication, or voluntary receipt of material that infringes on the copyrights, trademarks, trade secrets, or patent rights of any person or organization. Assume that all materials on the Internet are copyright and/or patented unless specific notices state otherwise.
* Transmission of any proprietary, confidential, or otherwise sensitive information without the proper controls;
* Creation, posting, transmission, or voluntary receipt of any unlawful, offensive, libellous, threatening, harassing material, including but not limited to comments based on race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs;
* Any form of gambling;
* Unless specifically authorized, the following activities are also strictly prohibited;
* Unauthorized downloading of any shareware programs or files for use without authorization in advance from the IT Department and the user’s manager,
* Any ordering (shopping) of items or services on the Internet,
* Playing of any games,
* Forwarding of chain letters,
* Participation in any on-line contest or promotion,
* Acceptance of promotional gifts.

Event logs shall record the following information:

* Type of Protocol accessed
* Website
* Category of website accessed
* Uploaded and downloaded file type and other details about the file
* User identification, if applicable
* Date and time of surfing

Monitoring results shall be reviewed on a daily basis with any exceptions and anomalies identified followed up during the review process.

For further information, refer to the XXXX IT Policy - “Internet Usage Management Policy”

**2.12.5 Responsibilities**

* All users are expected to understand this policy.
* Head, IT is responsible for implementing this policy
* Head, Information Security shall be responsible for enforcing and monitoring this policy
* Internal Audit – IS Audit is responsible for auditing the implementation of this policy.

**Roles and Responsibility Matrix**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Information Security** | **Information Security Forum** | **All Users** | **IT** |
| Ensuring policy is  fit for purpose | R/C | A | I | R |
| Annual policy review | R/C | A | I | C |
| Following the  policy | R | A | R | R |
| Communication of policy | R | A | I | R |

1. **Security Awareness and Training Policy**

**2.13.1 Overview**

IT security controls are a vital part of our information security framework but are not in themselves sufficient to secure all our information assets. Effective information security also requires the awareness and proactive support of all users, supplementing and making full use of the technical security controls. This is obvious in the case of social engineering attacks and frauds, for example, which specifically target vulnerable humans rather than IT and network systems.

Lacking adequate information security awareness and training, users are less likely to recognize or react appropriately to information security threats and incidents, and are more likely to place information assets in danger through ignorance and carelessness. It is therefore vital that XXXX have a security awareness program in place to ensure employees are aware of the importance of protecting sensitive information, what they should do to handle information securely, and the risks of mishandling information.

**2.13.2 Purpose**

To provide guidance and awareness to users on information security matters and motivation to fulfil their information security obligations

**2.13.3 Objectives**

The objective of this policy is to ensure that all users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support XXXX’s information security policy in the course of their normal work, and to reduce the risk of human error.

**2.13.4 Policy Details**

* All users in XXXX shall receive periodic Information Security awareness training to ensure they are aware of existing and new information security threats and concerns.
* All employees of the XXXX and, where relevant, contractors and third party users shall receive appropriate awareness training and regular updates in XXXX’s information security policies, procedures, guidelines, laws, regulations, contractual terms and plus generally held standards of ethics and acceptable use as relevant for their job function.
* An appropriate summary of the Information Security Policy must be given to all permanent and temporary employees, prior to their commencement of job role for the XXXX.
* All users shall be required to acknowledge, in writing or electronically, at least annually that they have read and understand the Information Security Policy
* All new employees shall attend the mandatory information security awareness training as part of induction before being granted access to the network or systems and at least annually for other employees. Where employee change jobs, their information security needs must be re-assessed and any new training provided as a priority
* Periodic training for the Information Security Officer is to be prioritized to educate and train in the latest threats and Information Security techniques.
* Users shall be held accountable for breaches in information security. It is therefore necessary for all employees of the XXXX to ensure they are up to date with the XXXX’s Information Security policy and abide by the guidelines.
* Information Security awareness shall be communicated to Personnel through:
* E-learning
* Training
* E-mails

**2.13.5 Responsibilities**

* All users are required to understand and comply with this policy at all times.
* Head, Learning and Development shall be responsible for implementing this policy.
* IT Service Desk shall be responsible for helping employees on basic information security matters, liaising with experts from functions such as Information Security, HCM, ERM, Legal and Compliance where necessary
* The Information Security Manager is accountable for running effective information security awareness and training program and is expected to ensure compliance to this policy
* Internal Audit – IS Audit is responsible for auditing the implementation of this policy.

**Roles and Responsibility Matrix**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Information Security** | **Information Security Forum** | **All Users** | **Learning and Development** |
| Ensuring policy is  fit for purpose | R/C | A | I | R |
| Annual policy review | R/C | A | I | I |
| Following the  policy | R | A | R | R |
| Communication of policy | A | A | I | R |

1. **Clear Desk & Clear Screen Policy**

**2.14.1 Overview**

This policy is to ensure that all sensitive and confidential information, whether it be on paper, a storage device, or a hardware device, is properly locked away or disposed of when a workstation is not in use. This policy will reduce the risk of unauthorized access, loss of, and damage to information during and outside of normal business hours or when workstations are left unattended

**2.14.2 Purpose**

To establish guidelines and procedures for reducing the risk of information theft / leakages caused by documents and computer screens being left unattended on a user’s desk.

**2.14.3 Objectives**

The objective of this document is:

* To improve the security and confidentiality of information
* To ensure that the XXXX’s information and information facilities are well protected

**2.14.4 Policy Details**

* All employees of XXXX are expected to tidy their desk of papers and any files in hardcopy or electronic form with personal/ confidential / sensitive information in them especially customer related records when leaving for the day / during short breaks.
* Each department shall provide a locker or filing cabinets for the purpose of complying with the clear desk policy. The desk locker or filing cabinets must be kept closed and locked when not in use or when not attended.
* Keys used for access to restricted or sensitive information must not be left at an unattended desk.
* Where applicable ensure any paper is shredded before being thrashed if it contains personal or confidential data.
* Employees where possible should not print off emails to read as this can result in information theft / leakage.
* Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer
* Laptops must be either locked with a locking cable or locked away in a drawer or cabinet when the work area is unattended or at the end of the workday.
* Compliance with the Clear desk policy shall be monitored periodically by Internal Audit / Internal Control / Branch Manager and defaulters shall be penalized / sanctioned appropriately.
* Internal Control shall conduct periodic sweep on all SBUs to measure compliance.
* Computers / computer terminals should not be left logged on when unattended and should be password protected.
* Computer screens should be angled away from the view of unauthorized persons.
* The screen is set to automatically lock when there is no activity for a period of five (5) minutes for windows system and twenty (20) minutes for Unix system/servers.
* CTRL+ALT+DEL is used to lock computer screens when leaving computer systems.
* Users must "log off" their computers when their workspace is unattended.
* Users must "shut down" their computers at the end of the workday.
* Passwords must not be left on sticky notes posted on or under a computer, nor written down in an accessible location.
* Whiteboards containing Restricted and/or Sensitive information should be erased.
* Personal computers and computer terminals should be switched off when not in use and should be password protected.

**2.14.5 Responsibilities**

* All users are required to understand this policy.
* Head, Internal Control is responsible for enforcing this policy.
* Head, Information Security is expected to ensure adherence to this policy
* Internal Audit – IS Audit is responsible for auditing the implementation of this policy.

**Roles and Responsibility Matrix**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Information Security** | **Information Security Steering Committee** | **All Users** | **Internal Control** |
| Ensuring policy is  fit for purpose | R/C | A | I | R |
| Annual policy review | R/C | A | I | I |
| Following the  policy | R | A | R | R |
| Communication of policy | R | A | I | R |

1. **Physical and Environmental Security Policy**

**2.15.1 Overview**

Physical and environmental security protects information, information systems infrastructure and facilities from physical and environmental threats. The term physical and environmental security refers to measures taken to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environment.

Physical and environmental controls are often overlooked but are very important in protecting information. Buildings and rooms that house information and information technology systems must be afforded appropriate protection to avoid damage or unauthorized access to information and systems. In addition, the equipment housing this information (e.g., filing cabinets, data wiring, laptop computers, and portable disk drives) must be physically protected.

**2.15.2 Purpose**

To establish guidance for mitigating the risks from physical and environmental threats.

**2.15.3 Objectives**

The objective of this policy is:

* To ensure the XXXX appropriately protects information systems equipment from physical and environmental threats.
* To ensure the XXXX appropriately protects buildings and rooms to prevent unauthorized access, damage, or interference to the information systems therein.

**2.15.4 Policy Details**

* All employees of XXXX, contractors, consultants and other visitors shall be required to have the XXXX’s approved identification badges on when on the premises of the XXXX.
* Entrance into the XXXX’s premises shall be restricted through the use of locks, keys, biometric locks, security guards, walls, card controlled entry or fingerprint recognition doors, manned reception desk and any other appropriate tools for restricting access.
* A security register shall be maintained at all the XXXX’s locations to access areas where equipment / devices supporting communication, data processing and storage are maintained.
* Physical access to the XXXX’s information systems facilities is to be restricted to authorized persons only. Authorization to enter restricted facilities is to be granted only when there is a business or technical reason for the person to enter the premises.
* Passes shall be zoned appropriately for secure areas (restricted zones) such as the IT Data Centre rooms as they require a higher level of security.
* Secure areas (restricted zones) must be protected with access control devices e.g. physical barriers, intrusion alarms, access-logging equipment such as card key systems and security cameras to ensure that only authorized personnel are allowed access.
* Access to sensitive or critical information processing facilities outside normal working hours must be specifically authorized and logged.
* Access rights must be updated regularly, based on the criticality of the information system.
* Visitors must be provided supervised and controlled access to secure areas in accordance with the physical access control procedures for visitors.
* All visitors shall declare their belongings like laptops etc. before entering restricted premises. The security officer must verify the declarations to prevent removal of the XXXX’s property from the building.
* Visitors are required to sign in to the visitors/contractors register at main reception.
* All visitors/contractors are to be given access cards permitting them to the floor for which they are visiting. One access card is issued per visitor/contractor
* If an unescorted person is seen around the office, staff are encouraged to politely challenge them.
* Under no circumstances, should a visitor be allowed to connect their own computer equipment to XXXX’s network, unless approved and authorized.
* Contractors access cards are given out upon completion of a request memo.
* Physical access rights must be revoked immediately upon termination/resignation of employees or completion of a consultation or vendor agreement.
* Data center, equipment rooms, and telecommunications closets must be protected from unauthorized or unnecessary access. The construction of data centers, equipment rooms, and telecommunication closets must take into account:
* Specifications developed as a response to potential threats to the asset.
* Specifications developed in accordance with the XXXX Information Classification and Control Policy.
* Vendor Specifications.
* All data centers, equipment rooms, and telecommunications closets must be locked when unattended.
* The office cleaners are an exception to the visitor rules set out above. They have been specifically vetted by the approved third party organization providing cleaning services to XXXX and as a result are the only visitors who are permitted to the non-restricted part of the office
* However, even in the case of the cleaners, extra vigilance should be applied with regard to information security. Sensitive information is placed in the locked cabinets during out-of-office hours. Employees are to ensure that all filing cabinets and sensitive areas are locked and the keys are stored in the appropriate location
* All Information Assets must be placed in a location commensurate with its criticality and its classification (See Information Classification and Control Policy).
* Environmental conditions, such as temperature and humidity, should be monitored for conditions, which could adversely affect the operation of information processing facilities
* Hazardous or combustible materials should be stored at a safe distance from a secure area.
* Backup equipment and media should be sited at a safe distance to avoid damage from a disaster affecting the main site
* Appropriate firefighting equipment should be provided and suitably placed.
* All information assets should have adequate maintenance plans and/or insurance based on the value of the asset.
* Information assets must not be moved from its location unless authorized by the asset owner.
* Information assets must be protected from power failures, electrical anomalies, fire, flood and other environmental hazards.
* Information assets must be protected from disruptions caused by failures in supporting utilities such as HVAC, water supply and sewage
* Critical Information assets must be supported by uninterruptible power supply (UPS). A backup power generating equipment should also be in place where possible.
* Power supply backup equipment including UPS’s, backup generators etc. must be subject to regular maintenance and testing.
* Power and telecommunications cables carrying data or supporting information services must be protected from interception or damage.
* Information assets must be maintained in accordance with appropriate mandatory procedures in place. As a minimum these procedures will recognize the criticality of the equipment and will comply with the vendor’s recommendations and specifications.
* Only authorized and qualified maintenance personnel must perform maintenance of the XXXX’s Information assets.
* Information assets used to support business activities outside of the XXXX’s premises must be made subject to the same type of authorization and security protection as that of on-site Information assets.
* All Information assets containing storage media (e.g., fixed hard drives) must be checked to ensure that any critical business information and licensed software are removed, securely overwritten or destroyed prior to disposal or re-use.

**2.15.5 Responsibilities**

* All users are required to understand this policy and put into action.
* Head, Safety and Security & Head, IT is responsible for implementing this policy.
* Head, Information Security is expected to ensure adherence to this policy
* Internal Audit – IS Audit is responsible for auditing the implementation of this policy.

**Roles and Responsibility Matrix**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Information Security** | **Information Security Steering Committee** | **All Users** | **IT / Safety & Security** |
| Ensuring policy is  fit for purpose | R/C | A | I | R |
| Annual policy review | R/C | A | I | I |
| Following the  policy | R | A | R | R |
| Communication of policy | R | A | I | R |

1. **Third Party Access Policy**

**2.16.1 Overview**

The Third Party Access Policy sets out the conditions that are required to maintain the security of the XXXX’s information and information systems when third parties are involved in their operation. This may occur in at least three distinct circumstances:

* When third parties (for example contractors) are involved in the design, development or operation of information systems for the XXXX. There may be many reasons for this to happen, including writing and installing bespoke software, third party maintenance or operation of systems, to full outsourcing of an IT facility;
* When access to the XXXX’s information systems is granted from remote locations where computer and
* network facilities may not be under the control of the XXXX
* When users who are not employees of the XXXX are given access to information or information systems.

Each of these circumstances involves a risk to the XXXX’s information, which should be assessed before the third party is granted. Such access must be subject to appropriate conditions and controls to ensure the risk can be managed.

**2.16.2 Purpose**

The purpose of this policy is to maintain the security of the XXXX’s information facilities that are accessed or provided by third parties.

**2.16.3 Objectives**

The objective of this policy is:

* To maintain the security of the XXXX’s information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.
* To ensure that all third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.
* To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.

**2.16.4 Policy Details**

* All third parties who are given access to the XXXX’s information systems, whether suppliers, customers or otherwise, must agree to follow the XXXX’s information security policies. The XXXX will require external suppliers of services to sign a confidentiality agreement to protect its information assets.
* The request must be sponsored by a department / unit in XXXX or and duly approved by the departmental head. Where hard copy access requests cannot be provided, email from the unit head will suffice.
* The System Owner will act as the sponsor for the Third Party where there is an approved need for Third Party Access. The System Owner (sponsor) will be expected to notify the IT service desk once the work has been completed.
* Third party access will be governed by formal written signed agreements. The Third Party Agreement must be signed by all third parties prior to access being given. See Appendix A – Third Party Access Form.
* Security controls will be agreed and defined in a contract with the third party as detailed in the agreement
* The owners of all third party links into XXXX’s systems must ensure that any systems connections they maintain do not affect the XXXX’s systems.
* All access will be using appropriate standards and technical solutions as defined by XXXX IT technical staff. This will be carried out in conjunction with the Information Security Manager (ISM).
* Third party users will be restricted to the minimum services and functions which are required to perform the specified tasks, as outlined by the System Owner (sponsor) in the original request for access.
* All information systems used to access XXXX systems must be patchable, up to date with the latest security patches and with up-to-date Virus signatures
* XXXX reserves the right to audit both the processes and systems of the third party, in so far as it relates to XXXX owned data. User’s systems may be audited to ensure no unauthorized activity is unnoticed. Any audit logs produced will be reviewed frequently.
* Appropriate protective monitoring techniques will be applied depending on the sensitivity of the data involved in the transactions.
* The Third Party is solely responsible for ensuring that any username and password that are granted remains confidential and is not used by unauthorized individuals.
* Third party connections must comply with requirements as stated in Service Level Agreements.
* Employees and third parties must use only the XXXX’s official email accounts, to conduct the XXXX’s business.
* XXXX may require Third Parties to undertake appropriate Information Security Awareness training sessions and to sign up to the XXXX Acceptable Usage Policy (AUP)
* The third party connection may be disconnected without notice if a breach of security is suspected or if the connection is interfering with normal operation of the production systems.
* The XXXX reserves the right to monitor activity and revoke access.
* On completion of the contract, the third Party must return all information facilities belonging to the XXXX.

**2.16.5 Responsibilities**

* All third party users are required to understand and comply with this policy at all times.
* System Owners or sponsors are responsible for any third party access.
* Head, IT and ISM is responsible for implementing this policy
* Internal Audit – IS Audit is responsible for auditing the implementation of this policy.

**Roles and Responsibility Matrix**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Information Security** | **Information Security Steering Committee** | **IT** | **All Third Party Users** | **System Owners** |
| Ensuring policy is  fit for purpose | R/C | A | R | I | I |
| Annual policy review | R/C | A | C | I | I |
| Following the  policy | R | A | R | R | R |
| Communication of policy | A | A | R | I | R |

1. **Remote Access Policy**

**2.17.1 Overview**

Remote access to corporate networks is essential to maintain productivity, but in many cases this remote access originates from networks that may already be compromised or are at a significantly lower security posture. While these remote networks are beyond the control of XXXX, we must mitigate these external risks to the best of our ability.

**2.17.2 Purpose**

To establish guidelines and procedures for managing remote access to the XXXX’s network in order to forestall uncontrolled or unauthorized access that may result in security breaches, or the misuse of the XXXX’s resources.

**2.17.3 Objectives**

The objective of this policy is:

* To improve the confidentiality, integrity and availability of information
* To ensure that the XXXX’s information and information facilities are well protected

**2.17.4 Policy Details**

* Remote access to the XXXX’s corporate network must be strictly controlled using approved tools.
* For devices connecting to the XXXX Corporate Network, the use of a two-factor authentication mechanism is mandatory to ensure secured tunnels to the network. This ensures stronger authentication, encrypted traffic and adequate security, while making it easier for users to make connections.
* All hosts that are connected to the XXXX’s internal network via remote access technologies, including personal computers, must use the most up-to-date endpoint security software.
* XXXX employees and contractors with remote access privileges must ensure that their XXXX-owned or personal computer or workstation, which is remotely connected to XXXX's corporate network, is not connected to any other network at the same time.
* At no time must any of the XXXX’s remote users provide their login details to anyone.
* Non-standard hardware configurations shall not be permitted on the XXXX corporate network.
* Personal equipment that is used to connect to XXXX's networks must meet the requirements of XXXX-owned equipment for remote access and must comply with this policy.
* Third party connections must comply with requirements as stated in Service Level Agreements.
* Employees and third parties must use only the XXXX’s official email accounts, to conduct the XXXX’s business.
* The XXXX reserves the right to audit compliance with this policy from time to time. Any disciplinary action, arising from breach of this policy, shall be taken in accordance with The XXXX’s Rules and Disciplinary Code as amended from time to time. Disciplinary action may ultimately lead to dismissal.
* Violations of this policy by users granted remote access to the XXXX’s information resources and network can result in the revocation of their access privileges and/or termination of their relationship with the XXXX.
* Unless specifically approved, any deviation from this policy is strictly prohibited. Any deviation from or non-compliance with this policy will be reported to the CISO & Head of IT.

**Guidelines**

* Control over remote access is necessary to prevent unauthorized access and abuse.
* Remote users are not permitted to divulge their login details to family members.
* An example of an external network that should not be connected to concurrently is a dial up connection.
* Examples of unofficial e-mail accounts include; Hotmail, Yahoo, etc.

**2.17.5 Responsibilities**

* All users are required to understand this policy and put into action.
* Head, IT is responsible for implementing this policy.
* Head, Information Security is expected to ensure adherence to this policy
* Internal Audit – IS Audit is responsible for auditing the implementation of this policy.

**Roles and Responsibility Matrix**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Information Security** | **Information Security Steering Committee** | **All Users** | **IT** |
| Ensuring policy is  fit for purpose | R/C | A | I | R |
| Annual policy review | R/C | A | I | I |
| Following the  policy | R | A | R | R |
| Communication of policy | R | A | I | R |

1. **Malware & Antivirus Policy**

**2.18.1 Overview**

In the context of information systems security, malicious software (malware) are computer programs which when executed in a computer system, could perform some type of harmful activity on the infected hosts, such as clogging hard disk space or CPU time, accessing private information, corrupting data, displaying unsolicited political or humorous messages on the user's screen. Computer malware include computer viruses, worms, Trojan horse programs, rootkits, key loggers, adware, spyware, etc.

Malwares can be transmitted via e-mails or instant messaging attachments, downloadable internet files, USB memory devices and other removable (storage) media etc. Malicious software programs are very harmful to information assets.

This policy document gives guidance and direction on minimizing the risk of a computer malware infection in the XXXX and the use of antivirus software deployed in XXXX.

**2.18.2 Purpose**

This document aims at providing a set of guidelines that shall govern the effective prevention, detection and recovery from malicious software (malware) infection within the XXXX’s information systems space.

**2.18.3 Objectives**

The objective of this policy is to ensure that:

* the need for antivirus protection and malware detection is communicated effectively
* specific requirements for protecting commonly affected systems against malware attacks are defined
* the XXXX’s assets and information facilities are adequately protected from malware
* Early detection of malware prior to any widespread attack against the XXXX’s networks, computers and servers takes place.

**2.18.4 Policy Details**

It is the policy of the XXXX that all access to information and information processing facilities is protected by antivirus software.

* The approved enterprise anti-virus solution for windows operating systems clients and servers in the XXXX is Microsoft Forefront Endpoint Protection; hence only this solution shall run on systems on the network. The use of other antivirus solutions is PROHIBITED unless approved by Head, IT
* Any activity with the intention to create and/or distribute malicious programs into the XXXX’s networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) is prohibited in accordance with the Acceptable Use Policy.
* Users must not disable or in any other way reconfigure antivirus software running on systems in such a way as to impair its normal functionality
* Laptop users who operate their laptops on and off the network must regularly connect to the network to ensure that the anti-virus software virus definitions remain up-to-date. Failure to do so could result in unnecessary virus outbreaks.
* Installation/use of unauthorized software on the network is strictly prohibited. Unauthorized use, in addition to breaching copyright requirements, could introduce malicious software into the network.
* If an employee receives what he/she believes to be a virus, or suspects that a computer is infected with a virus, he/she must report such incident to the IT Department immediately by e-mailing ITservicedesk@XXXX.com. Report the following information (if known): virus name, extent of infection, source of virus, and potential recipients of infected material.
* Users must not accept and/or open email attachments, macros and other executable files from unknown, untrustworthy or suspicious sources.
* Users are advised to avoid direct disk sharing with read/write access. Users must always scan any removable media for viruses before using it.

**CONTROLS**

* Supported anti-virus software must be installed and updated at regular intervals.
* Anti-virus software and virus pattern files or definitions must be kept up-to-date.
* Virus-infected computers must be removed from the network until they are verified as virus-free.
* All software to be deployed/ installed on the XXXX’s information system must be reviewed and confirmed to be virus free before deployment. This requirement applies to in-house and off-the-shelf software, maintenance/customization releases (internally or externally developed), updates and patches, etc.
* ESD is responsible for ensuring that anti-virus software is updated at regular intervals, and computers are verified as virus-free.
* Any activity intended to create, introduce or distribute malicious programs within XXXX networks is prohibited.
* Antivirus software shall be actively running and must not be disabled or altered by users.
* Antivirus software shall be capable of protecting against, detecting and removing all types of malicious software.
* It is required that the antivirus software is kept up to date, and a version review conducted quarterly.
* The antivirus database must be set to automatically update.
* Periodic antivirus scans are required in accordance with regulatory and information security requirements.
* In the event of malware causing loss, an investigation must be conducted, where forensic methods may be used to satisfy legal and regulatory requirements.
* Antivirus logs must be retained for at least one year.
* Processes must be in place to restore the last three months of logs for forensic analysis.

**2.18.5 Responsibilities**

* ESD (Enterprise Servers and Desktops) shall be responsible for the following: Only appropriately skilled staff may administer antivirus software, using personal user accounts with administrator rights, where accountability and traceability are required. Group or shared Antivirus administration accounts are explicitly prohibited.
* Administration and operation of the XXXX’s antivirus software.
* Applying any updates to the services it provides that are required to defend against threats from viruses.
* Install anti-virus software on all XXXX owned and installed desktop workstations, laptops, and servers.
* Assist employees in installing anti-virus software according to standards on personally-owned computers that will be used for business purposes. XXXX will not provide anti-virus software in these cases.
* Take appropriate action to contain, remove, and assist in recovery from virus infections. In order to do so, IT may be required to disconnect a suspect computer from the network or disconnect an entire segment of the network.
* Head, Information Security is responsible for enforcing policy for compliance.
* IS Audit - Responsible for auditing the implementation of this policy.

**Roles and Responsibility Matrix**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **ESD** | **Information Security** | **Information Risk Committee** | **All Users** |
| Ensuring policy is  fit for purpose | R | R/C | A | I |
| Annual policy review | C | R/C | A | I |
| Following the  policy | R | R | A | R |
| Communication of policy | R | R | A | I |

**Exhibit B**

Attachments file types blocked by default on the official email client (Outlook) includes:

|  |  |
| --- | --- |
| **File extension** | **File Type** |
| .exe | Executable file |
| .pps | Power Point slide show |
| .mov | Multi Media file |
| .mpeg | Video file |
| .mp4 | Mpeg4 video file |
| .mp3 | Mpeg audio stream file |
| .wav | Sound file |
| .avi | Audio-Video Interleave |
| .mps | Mpeg-1 audio & video |
| .wmv | Window media video |

1. **Vulnerability Management Policy**

**2.19.1 Overview**

In the context of information systems and security, vulnerability is defined as a weakness which allows an attacker to exploit or compromise information systems. Vulnerability management is an essential component of any information security program and the process of vulnerability assessment is vital to effective vulnerability management. Vulnerability assessment is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system. An effective vulnerability management system is vital to ensure adequate protection of an organization’s information system.

**2.19.2 Purpose**

To establish guidelines and procedures conducting vulnerability assessments and penetration tests against the XXXX's assets.

**2.19.3 Objectives**

The objective of this document is to protect the confidentiality, integrity and availability of the XXXX’s information systems

* + 1. **Policy Details**

**General**

* The XXXX shall engage an external vendor to carry out periodic Vulnerability Assessments and Penetration Testing on targeted information system assets of the XXXX.  Reports of these assessments must be documented and approved by the CISO with the concurrence of Head, IT.
* The Vulnerability management shall be conducted once in a fiscal financial year by the external vendor and when there is significant infrastructural or environmental change (PCIDSS 11.3) and (ISO 27001:2013 A12.6)
* Only approved vulnerability scanning tools shall be used on the XXXX’s information systems. The Head, Information Security shall be solely responsible for the approval of vulnerability scanning tools to be used in the XXXX. If there is a need to use other scanning tools, such tools must have documented justifications and require the approval of the Head, Information Security.
* Information Security & IS Audit shall conduct quarterly vulnerability assessment.
* Installation/use of unauthorized software on the network is strictly prohibited.
* Only Information Security and IS Audit personnel have the approval to conduct vulnerability scans on the XXXX’s information systems. Any other staff seeking to conduct scans on the systems must obtain an approval from the Head, Information Security.
* The scope of the activities that will be involved in test include but not limited to:
* Network infrastructure (wired & wireless)
* Operating Systems
* Web Applications;
* Extranet;
* Perimeter Security Devices; and
* Applications
* Vulnerability assessment will follow the Open Web Application Security Project (OWASP) criteria for testing. Listed below are the OWASP Top 10 Web Application Security Risks:
* Injection
* Broken Authentication and session management
* Cross-site scripting (XSS)
* Insecure direct object references
* Security misconfiguration
* Sensitive data exposure
* Missing function level access control
* Cross-site request forgery (CSRF)
* Using components with known vulnerabilities
* Invalidated redirects and forwards
* The report of this exercise shall be a documentation of all findings, gaps in security measures and suggested countermeasures. The report shall serve as a means of remediation and improvement on the XXXX’s security defenses.
* Vulnerability assessment reports may contain sensitive XXXX information, as such; all reports must be treated as confidential. Also a non-disclosure agreement must be signed with an external party before commencement of vulnerability scanning activities.
* All new information systems deployed in the XXXX – applications (in-house and off the shelf), network infrastructure (wired and wireless), etc. – must be scanned for vulnerabilities and all identified vulnerabilities remediated prior to migration to operational (live) environment. In the same vein, all major changes to the XXXX’s information system shall undergo vulnerability scanning and all identified vulnerabilities remediated prior to migration to the operational environment.
* Information systems that appear to be causing disruptive behavior on the network may be scanned using non-intrusive methods by the relevant Information Security officer to investigate the source of the disruption.
* As part of their job function, the Information Security team shall periodically visit security website such as SANS.org, CERT.org and CISecurity.org to keep abreast of evolving trends in information security especially as it affects information systems deployed in the XXXX.

**Patch Management**

* XXXX will update and apply security patches to critical IT systems within 30 days of patch release to address information security vulnerabilities.
* Regular patching procedures are defined and follow a designated process.  Emergency patches will be applied when necessary, requiring the approval of the CISO.
* XXXX will implement a process to keep up to date with current security vulnerabilities and associated patches.
* In addition, the Information Security department will regularly check vendor sites and communications for patches and updates to critical software systems.

**Remediation and Priorities**

* At the conclusion of each assessment, a remediation plan/report shall be prepared and sent to the Head, Information Security. The report shall summarize the following:
  + List of Vulnerabilities: All discovered vulnerabilities, the severity, and the affected information systems.
  + Remediation Steps: Each of the vulnerabilities listed shall have detailed information on how the vulnerability shall be remediated or eliminated with completion timelines.
* The Information Security team shall produce a documented semi-annual vulnerability assessment report, which includes details of all outstanding vulnerabilities at year end. This report shall be submitted to the Information Security Forum. The vulnerability assessment report may also contain vulnerabilities discovered by other teams.
* Vulnerabilities discovered on information systems on the XXXX’s network shall be remediated and /or mitigated based on the schedule in the table below:

|  |  |  |  |
| --- | --- | --- | --- |
| **S/N** | **VULNERABILITY RATING** | **DESCRIPTION** | **REMEDIATION INTERVAL** |
| 1 | High/Critical | These are vulnerabilities through which an attacker could gain access to the system at the administrator level or could possibly access sensitive information stored on the system. | Vulnerabilities shall be fully addressed within 15 calendar days of discovery. |
| 2 | Medium | These vulnerabilities may allow an intruder to gain access to specific information stored on the host, including security settings. They can also allow intruders gain access to information that may be used to compromise the host in the future. | Vulnerabilities shall be addressed within 45 calendar days of discovery |
| 3 | Low | Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions. | Low level vulnerabilities shall be addressed within 180 calendar days of discovered |
| 4 | Informational | These vulnerabilities do not pose an immediate threat to the XXXX’s systems. They are mostly weaknesses that may allow an intruder access to information that may be used in the future to compromise the host | Vulnerabilities in this category shall be given attention after the higher priority vulnerabilities have been addressed |

* + 1. **Responsibilities**
* All users are required to understand this policy and are responsible for ensuring the safety and security of the XXXX’s systems and the information that they use or work with.
* Information Security is responsible for implementing this policy.
* Internal Audit – IS Audit is responsible for auditing this policy.

**Roles and Responsibility Matrix**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Information Security** | **Information Security Steering Committee** | **IS Audit** | **IT** |
| Ensuring policy is  fit for purpose | R/C | A | I | R |
| Annual policy review | R/C | A | I | I |
| Following the  policy | R | A | R | R |
| Communication of policy | R | A | I | I |

1. **Information Security Incident Management Policy**

**2.20.1 Overview**

Incident management describes the activities of an organization to identify, analyze, and correct hazards to prevent a future re-occurrence. The Information Security Incident Management Policy addresses intrusion, compromise and misuse of information and information resources, and the continuity of critical information systems and processes.

This policy shall ensure that information security events and weaknesses associated with information systems are documented and communicated in a manner that allows timely corrective actions. Thereof, this shall serve as inputs to preventive actions that will safeguard the confidentiality, integrity and availability of XXXX’s Information assets.

**2.20.2 Purpose**

The XXXX has a responsibility to monitor all incidents that occur within the organisation that may impact on the confidentiality, integrity, availability or accountability of information. All incidents need to be identified, reported, investigated and monitored. This Policy defines the requirements to ensure information security management incidents are reported and managed effectively within XXXX.

The ultimate aim of incident management is to prevent or minimise harm or detriment to customers or employees. Others include

* To define appropriate mechanisms for responding to information security incidents
* To ensure that information asset owners are appropriately identified and are informed of security incidents
* To assign responsibilities for the information security incident response management process
* To ascertain the seriousness and impact of an incident
* To identify any vulnerability created by an information security incident
* To estimate the resources that are required to mitigate the incident.
* To ensure that proper post-incident reporting occurs and that procedures are reviewed and adjusted in order to mitigate risk and prevent future incidents.

**2.20.3 Objectives**

The objective of this policy is to ensure:

* Proper recognition, management, and communication of security events and weaknesses through a formal process.
* Information security events and weaknesses associated with information systems are documented and communicated in a manner that allows timely corrective action to be taken and the lessons learned thereof serve as inputs to preventive actions.
* The quick and precise assessment of security incidents applying most appropriate response.
* Shortened recovery times to incidents and minimized business disruption.
* The confidence to proceed with a disciplinary action using proper procedures and processes to gather evidence in response to the incident.
  + 1. **Policy Details**
* All users and Suppliers shall be aware of the requirements for reporting incidents, and weaknesses and shall adhere to the processes set out in this document. Kindly refer to the Incident Management Procedure.
* All information Security incidents and weaknesses are to be logged in a timely manner for appropriate action to be taken in order to reduce the impact of an information Security incident.
* Information Security Incidents must be reported to outside authorities whenever this is required to comply with legal requirements or regulation. This may only be done by authorized persons.
* InfoSec, IT, HCM and General Services shall monitor, analyse and report on events to determine any changes in risks affecting the confidentiality, integrity and availability of information assets.
* Employees are expected to remain vigilant at all times for possible fraudulent activities
* Incident response plans shall be tested on an annual basis.
* Users with security breach responsibilities shall be provided with appropriate training.
* All evidence, ideas, and hypotheses about information systems crimes experienced by the XXXX, including possible attack methods and perpetrator motivations, must be treated as restricted and "legally privileged" information.
* All known vulnerabilities in addition to suspected or known violations must be communicated in an expeditious and confidential manner to Information security department. Unauthorized disclosures of the XXXX’s information must additionally be reported to Internal Control unit.
* Reporting security violations, problems, or vulnerabilities to any party outside the XXXX without the prior written approval from CISO is strictly prohibited.
* Any attempt to interfere with, prevent, obstruct, or dissuade a staff member in their efforts to report a suspected information security problem or violation is strictly prohibited and a cause for disciplinary action. Any form of retaliation against an individual reporting or investigating information security problems or violations is also prohibited and a cause for disciplinary action.
  + - First level investigation of Information Security incidents shall be carried out by Information security unit with escalation to the Incident Response Team (IRT).
    - The use of information systems must be monitored regularly with all unexpected events recorded and investigated. Such systems must also be periodically audited with the combined results and history strengthening the integrity of any subsequent investigations.
    - Information relating to Information Security incidents may only be released by authorized persons

**2.20.5 Controls**

**Incident Response**

Systems, alerts and vulnerabilities shall be monitored as a method of detecting information Security incidents. The XXXX’s priorities for handling information security incidents shall be established. Processes to handle different types of information security incident shall include:

* Investigating and recording the cause of the incident
* Containment
* Planning and implementation of corrective action to prevent recurrence, if necessary
* Communication with those affected by or involved with recovery from the incident
* Reporting the action to an appropriate authority such as the police or regulator
* Audit trails and similar evidence to be collected and secured

Actions to recover from security breaches and to correct system failures shall be carefully and formally controlled.

**Reporting information security incidents**

* All employees and users are responsible for promptly reporting suspected or known security incidents, in accordance with the Information Security Incident Management policy. Security incident breaches can be reported in various ways such as:
* Using the Global Service Desk – Logging security incidents on the **IS SECURITY INCIDENTS** folder. **Note: Only Information Security Incidents should be logged**.
* Send a mail to [ITservicedesk@XXXX.com](mailto:ITservicedesk@wemabank.com) / [infosec.office@XXXX.com](mailto:infosec.office@wemabank.com)
* All suspected high severity incidents, including those involving possible breaches of the XXXX’s information, must be reported directly to the Chief Information Security Officer (CISO) as quickly as possible.
* All Information Security incidents and weaknesses shall be reported immediately to the Information Security Team.
* All users shall be made aware of their responsibility to report any information security events and the process for doing so.
* IT shall review and monitor all issues reported via the Global Service Desk and identify possible information security incidents, events and weaknesses. These events and incidents shall be reported directly to the Information Security Team.
* General Services shall review and monitor all security and building issues reported and identify possible information security incidents, events and weaknesses. These events and incidents shall be reported directly to the Information Security Team.
* Suitable feedback processes shall be followed to ensure that those reporting information security events are notified of results after the issue has been dealt with and closed.
* Where appropriate the incident needs to be escalated to the appropriate authority. The Information Security Team will maintain a list of all the relevant Authorities and their contact details.
* Standard information security event reporting records shall be created to support the reporting action and to facilitate the collection of all relevant information.
* Prior to reporting the event, users shall note all important details but not carry out any action of their own, for whatever purpose or no matter how well intentioned.
* Users who are found to be involved in, or at fault for, security breaches shall be dealt with in accordance with the XXXX’s disciplinary policy.
* Processes used by the Information Security Team shall ensure that any evidence is collected as soon as possible after the security event, and in a forensically sound way.
* Where necessary, a defined incident owner will be appointed to manage the overall response to the event.

**Containment**

Actions shall be taken to minimise the impact of the incident by containing and isolating the affected components. It is an immediate priority to ensure that the incident is contained and cannot replicate to other areas of the business.

**Risk Assessment and root cause analysis**

* In parallel to the containment phase, and when sufficient information is obtained, a risk assessment shall be performed. The risk assessment shall be performed in alignment with best practices and based on knowledge of the systems and controls in place. It shall consider the risks not only to the XXXX, but also to the customer, business partners or any other relevant parties.
* A root cause analysis shall be performed to ensure that all issues are addressed. This shall be approved by Information Security.

**Learning from security events, incidents and weaknesses**

* Information security incident reporting and recording mechanisms shall enable the types, volumes and costs of information security incidents to be analysed.
* The information gained from the analysis of information security incidents shall be used to identify recurring or high impact incidents. All industry developments shall also be incorporated in order to keep the plan current and be able to react to emerging threats and security trends.
* The analysis of information security incidents shall indicate the need for enhanced or additional controls to limit the frequency, damage and cost of future occurrences, or to be taken into account in the security policy review process.
* Reoccurring or high risks shall be reported to the Information Security Forum, when appropriate.

**Collection of Evidence**

Where a follow-up action against a person or organization after an information risk incident involves legal action (either civil or criminal), evidence should be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

* The XXXX’s Legal Department shall provide advice on the rules for evidence that apply in any given situation and any actions that need to be taken where the incident cross borders into other jurisdictions.
* The XXXX’s Legal Department shall be involved in the early stages of any investigation in order to assess whether legal action may ensue and, hence, the evidence required.

**Notifications**

Upon the conclusion of investigation, the XXXX must understand its notification requirements. The XXXX may be required to inform business partners, individual customers and the Central XXXX of Nigeria or other regulatory bodies (e.g. Acquirer and Card Brand). A consideration shall be made on who to notify and how. This is the responsibility of the Information Security Forum

**2.20.6 Responsibilities**

* The XXXX’s Information Security Team shall be responsible for ensuring that:
* Formal event reporting and escalation processes are developed and maintained
* All users are made aware of the processes for reporting the different types of event and weaknesses that might have an impact on the security of the XXXX’s assets
* IT shall be responsible for monitoring technology and IT service issues and identifying and reporting information security incidents and weaknesses, identified via the various control mechanisms in place in Production/Development environments.
* General Services shall be responsible for monitoring building and physical security issues and identifying and reporting information security incidents and weaknesses.
* All users shall be responsible for reporting any information risk events and weaknesses as quickly as possible to Information Security.
* Suppliers shall be responsible for supporting and delivering processes, reporting incidents and weaknesses in a timely manner through a formal and agreed reporting process.
* IRT - The Incident Response Team is responsible for managing the XXXX’s response to an incident
* Internal Audit– IS Audit is responsible for auditing the implementation of this policy.

**Roles and Responsibility Matrix**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Information Security** | **IT, General Services** | **Information Security Steering Committee** | **All Users** | **IRT** |
| Ensuring policy is fit for purpose | R | R | A | I | R |
| Annual policy review | R | C | A | I | I |
| Following the policy | R | R | A | R | R |
| Communication of policy | R | R | A | I | R |

* + 1. **Types of incidents**

An incident is defined as any event that affects or threatens the confidentiality, integrity, availability or accountability of information. In other words, an incident is any event that implies harm or the attempt to harm.

Incidents may be identified as a result of the following activities:

* by routine systems monitoring, such as Intrusion detection system (IDS), Intrusion prevention system (IPS), file integrity monitoring (FIM) and firewall monitoring systems, or other technical monitoring
* by users noticing an extraordinary or unusual event
* through reports to Information Security or other security teams
* by customer complaints or queries
* by a department’s exceptions report
* by IT during system maintenance

An Information Security Incident includes, but is not restricted to, the following:

* The loss or theft of data or information
* The transfer of data or information to those who are not entitled to receive that information
* Attempts (either failed or successful) to gain unauthorised access to data or information storage or a computer system
* Changes to information or data or system hardware, firmware, or software characteristics without XXXX knowledge, instruction, or consent
* Unwanted disruption or denial of service to a system
* The unauthorised use of a system for the processing or storage of data by any individual

**Business Incident Management Process Flow**



### Backup and Recovery Policy

**2.21.1 Overview**

Backups of data is a vitally important part of any recovery strategy. When treated as an afterthought or merely as a checkbox item on an annual audit, the risks of losing critical data are significantly elevated. For these reasons, it is important to establish a disciplined regimen of data protection defined by a set of clear backup and recovery policies that can be closely followed and monitored.

**2.21.2 Purpose**

To establish guidelines and procedures for managing backup & recovery of data

* + 1. **Objectives**
* To protect against loss of data.

**2.21.4 Policy Details**

* Backup of data from critical business applications shall be performed daily by the system administrator / delegate
* Data shall be backed up to tape or disk and taken to an offsite location at least once every 2weeks
* Information system owners shall ensure that adequate backup and system recovery procedures are in place for all critical data
* Backup of critical business data shall be restored and validated by IT & Compliance at least once every quarter
* IT Management shall ensure that safeguards are in place to protect the integrity of the data files during the recovery and restoration of data files, especially where such files may replace more recent files
* Data on backup tapes / disk shall be duly protected to ensure data integrity when backup tapes or disk are being taken to an offsite location.
* Critical but non-database documents must be backed up unto the fileserver by document owners. SBU Heads must ensure compliance to safeguard critical documents from residing on personal laptops and computers.
* Restore of backed up data should be carried out half-yearly first in a test and controlled environment and then replicated to a live environment.

**2.21.5 Responsibilities**

* All members of staff are expected to understand this policy
* IT support staff are expected to understand and comply with this policy
* Head, IT & Digital Compliance is responsible for enforcing this policy
* Internal Audit– IS Audit is responsible for auditing the implementation of this policy.

### Business Continuity Policy

**2.22.1 Overview**

Business Continuity Management (BCM) is a process that enables the XXXX to proactively identify and plan to minimise the impact of risks that could affect its objectives, operations and information assets. The business continuity framework will provide for the development of processes, and the availability of information resources that ensure the continued achievement of the XXXX's critical business objectives.

It will provide a robust framework that allows the XXXX to:

* better understand risks;
* realize the potential for different types of disruption that may impact critical business objectives; and,
* to better plan for management of those disruptions and to put in place business improvement now, to reduce the likelihood and/or consequence of significant disruption

**2.22.2 Purpose**

The purpose of this section is to ensure the continuous delivery of key business processes in event of a disaster. It is different from disaster recovery planning since it is proactive and concentrates on everything that is needed to continue the key business processes.

* + 1. **Objectives**

The overall objective of this document is to maintain operations in a safe and available manner, where feasible. This is to ensure that in the event of an incident or crisis situation:

* There will be a logical recovery of the business
* Impacts will be kept within acceptable levels as defined by the business department representatives
* Business will continue as usual, as far as possible
  + 1. **Policy Details**
* Operational Risk Management Unit is required to initiate a Business Continuity Plan (BCP) XXXX wide. The Business Continuity Plan is to be kept up to date periodically.
* The Business Continuity Plan is to be periodically tested by Operational Risk Management to ensure that the Management and staff understand how it is to be executed. All tests and events are to be recorded.
* Comprehensive Business Continuity Plans for the departments are maintained and managed by the Operational Risk Department in conjunction with the respective departments.
* Business Impact Analysis for identified critical processes and activities shall be conducted and recorded by the Operational Risk Management unit for all business activities, services and assets; this also details the Business Continuity teams required should an event occur.
* All staff must be made aware of the Business Continuity Plan and their own respective roles by various business unit Heads.
* The Information Technology Unit / Information Technology Support must implement all hardware, software, policy, and related procedures consistent with the approved standards and with a focus to emergency/disaster support. Non-standard systems are unacceptable.
* The Information Technology Department are responsible for ensuring that the Disaster Recovery documents, processes and testing for each identified critical systems are in place and up-to-date.
* All staff must promptly report all information security alerts, warnings, suspected vulnerabilities, and the like that could lead to a disruption of business activities to the ORM or Information Security Unit.
* Periodically, Information Security unit must review all information security vulnerabilities advisories issued by Trusted Organizations such as Microsoft, Manufacturers of Security Systems and Regulators.

**2.22.5 Responsibilities**

* All staff will be responsible for understanding and complying with this policy.
* Head, Operational Risk shall be responsible for implementing this policy.
* The Operational Risk Management (ORM) Unit is responsible for:
  + reviewing the BCPs of business units
  + advising business units of current BCM best practice
  + developing and circulating BCM guidelines
* Head, Information Security is responsible for ensuring compliance with this policy
* Internal Audit – IS Audit is responsible for auditing the implementation of this policy.

**Roles and Responsibilities Matrix**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Information Security** | **Information Security Forum** | **All Users** | **Operational Risk Management** |
| Ensuring policy is  fit for purpose | R/C | A | I | R |
| Annual policy review | R/C | A | I | I |
| Following the  policy | R | A | R | R |
| Communication of policy | A | A | I | R |

### Cryptography Policy

**2.23.1 Overview**

The protection of electronic information and access to information systems is vitally important - especially with the ever increasing and greater demand. Cryptography provides an enhanced level of security from unauthorized access, disclosure or use when information is being transmitted or kept in storage. The Cryptography Policy sets out when and how encryption should (or should not) be used. It includes protection of sensitive information and communications, key management, and procedures to ensure encrypted information can be recovered by the XXXX if necessary.

**2.23.2 Purpose**

This policy addresses cryptographic techniques used for the protection of information and also define standards for managing the lifecycle of encryption keys.

* + 1. **Objective**
* To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.
  + 1. **Policy Details**
* Hardware cryptography is utilised via Hardware Security Module (HSM) for all ATM machines deployed by XXXX.
* Cryptography shall be implemented for software when applicable. The Head, Information Security prior to use, must approve all encryption products, processes, and standards.
* Sensitive information shall be protected against unauthorised disclosure when it is stored on electronic storage media if the information cannot be protected using sufficient physical or logical controls, and the information is at risk of being compromised or stolen. Utilisation of USB devices is prohibited for the storage of information.
* If a server, workstation, or laptop contains sensitive information, then that data shall be encrypted if the information cannot be protected using sufficient physical or logical controls, and the information is at risk of being compromised or stolen.
* Any data sent off-site for storage should be accorded the same level of security as the on-line data.
* To protect from unauthorized disclosure, modification, or loss, the entire electronic storage media should be encrypted along with supervisor password before sending off-site. All backup media shall be stored in secure container. The access privilege to backup and restore files and directories shall be limited to authorised personnel only.
* Split knowledge and dual control of keys shall be used to eliminate the possibility of one user having access to the whole key.
* Keys must be accessible only to key custodians to enable their effective use. No other personnel are allowed access to the keys except the appropriate security key officer.
* Keys must be stored securely and protected against both disclosure and misuse and exist in the fewest possible locations or forms.
* Old keys that are no longer used or needed must be replaced and destroyed to ensure that the keys can no longer be used.
* Encryption keys shall be generated only by designated personnel that are referred to as ‘Key Custodians’.
* Key Custodians shall be selected from different departments and they must be full time employees that has worked in the XXXX for at least one year.
* Subsequent access to retrieve any key part is granted only to the Key Custodian that generated it.
* The Internal Control department manages the selection of Key Custodians and maintains a list of persons assigned.
* The XXXX’s Management has the overriding authority to reassign access to Keys if the original custodians are not available.

**2.23.5 Responsibilities**

* IT will be responsible for understanding and complying with this policy.
* Key Custodians (selected from different departments – E-business & Payments, IT, Internal Audit, Internal Control, Branch BSM, and ATM Regional Engineers) shall be responsible for the generation of keys.
* Head IT shall be responsible for process coordination of this policy.
* Head, Information Security is responsible for ensuring compliance with this policy
* Internal Audit – IS Audit is responsible for auditing the implementation of this policy.

### Supplier Control Policy

**2.24.1 Overview**

This policy outlines all the requirements in place to ensure the integrity and management of all suppliers with Information Security requirements being taken into account to secure XXXX’s information infrastructure and facilities that are supplied by an external entity.

**2.24.2 Purpose**

The purpose of this document is to define the requirements for relationship with all suppliers and partners.

* + 1. **Objectives**

To ensure the provision of seamless and quality service of suppliers.

**2.24.4 Policy Details**

* All external suppliers who are contracted to supply services to the XXXX, must agree to follow the Information Security policy of the XXXX.
* Mutual nondisclosure/confidentiality agreements must be signed when interaction with a third party begins.
* XXXX will check the implementation of contracts and vendor selections, monitor compliance, and manage changes to ensure that suppliers meet all requirements.
* All suppliers will be informed of the requirement to adhere to XXXX’s information security policies. This provision is included in all future contracts and appended to existing contracts with the supplier.
* Access to XXXX’s information and the customer data held on our services is subject to the information security policies in place.
* All major suppliers are evaluated on an annual basis.
* The SLA’s with business critical suppliers are fully reviewed. Where practical an audit or evaluation report may be sought from these suppliers to the effectiveness of their Information Security Management System (or equivalent).
* The Top Management team are the only personnel permitted to approve new suppliers. Appropriate information security awareness training has been given to all levels within XXXX.
* When information or data is to be transferred between XXXX and a supplier this is conducted as per the Information Transfer Policy.
* An inventory of data transfers to external suppliers must be maintained by all business areas, kept current and regularly reviewed, in accordance with a formal documented process.
  + 1. **Responsibilities**
* ITAS and General Services, Information Security team will be responsible for understanding and complying with this policy.
* Head IT shall be responsible for implementing this policy.
* Head, Information Security is responsible for ensuring compliance with this policy
* Internal Audit – IS Audit is responsible for auditing the implementation of this policy.

### Information Transfer Policy

**2.25.1 Overview**

On many occasions, information is transferred between departments, to third-party service providers, to other public bodies, commercial organisations and customers. This is done using a wide variety of media and methods, in electronic and paper format. In every transfer there is a risk that the information may be lost, misappropriated or accidentally released.

For reasons such as confidentiality or data protection, and to maintain the trust of our customers and stakeholders, it is essential that the transfer of information is being protected. This policy outlines the responsibilities attached and the minimum security requirements for secure information transfer.

**2.25.2 Purpose**

This policy sets out the processes to be followed in all XXXX communications both within and outside the XXXX. These include encrypted drive handling, post, telephone, electronic communications and hand delivery. XXXX needs to maintain an efficient communications policy so that relevant information is processed and stored.

* + 1. **Objectives**

To maintain the security of information and software transferred within the XXXX and with any external entity

* + 1. **Policy Details**

Incoming Post

* All incoming post addressed to XXXX are received at the reception/front desk. Mail/Posts are sorted and dispatched to the appropriate XXXX location. Mails/Post are acknowledged, date stamped and passed to the relevant departmental member of staff or unit unopened.
* Customer Service executives at the front desk do not open Mails/Post. Post marked for the attention of an individual will be passed directly to the relevant member of staff unopened. Any post marked as ‘Private and confidential’ will be treated as such.
* Junk mail should be discarded.
* In the absence of the receptionist a designated member of staff will deal with incoming post.
* Particular attention should be paid to urgent and important communications.
* All cheques received by post should be immediately passed to the Finance Department to be date stamped and logged

Outgoing post

* All outgoing correspondence should be written in correct English, should be free from errors and neatly typed and bearing XXXX logo.
* Any Private and Confidential correspondence should be clearly marked as such.
* Large mail outs requiring mail sacks must be kept in the collation area when they will be moved to the post area for collection.

Telephone Messages

* In all cases take down the name of the caller, his/her telephone number, company’ name (if relevant) should be taken down in clear and understandable message.
* Telephone calls should be made being aware of the sort of information being discussed within surroundings.

Electronic Media

* When electronic media is to be sent via the postal service, all confidential documents contained on the media (be it CD/DVD or a Pen Drive) are to be password protected.
* Public electronic media is sent through normal postal channels.
* All electronic media is adequately protected to ensure no damage can ensue during transportation.

Hand Delivery

* When media is in electronic format all documents shall be virus checked prior to delivery.
* All media will be securely handled as per the Mobile Equipment Policy. This includes hard copy media.
* Media will only be exchanged in a secure manner. This means in the client’s premises / office. A signature is required for the receipt of any information delivered in this manner.
* All electronic media is adequately protected to ensure no damage can ensue during transportation.
* Customer information (such as customer account details) must not be sent via the Internet, unless approved and authorized encryption is employed.
* XXXX’s employees are required to use professional and ethical judgment while exchanging internal information / opinions / XXXX’s Intellectual Property or any other information on public forums. The user holds responsibility for any actions that are unethical and hampers the reputation and security posture of XXXX. In case of unacceptable information transfer or exchange, XXXX may take disciplinary actions as needed.

**2.25.5 Responsibilities**

* All staff will be responsible for understanding and complying with this policy.
* Head IT Control shall be responsible for implementing this policy.
* Head, IT & Digital Compliance is responsible for ensuring compliance with this policy
* Internal Audit – IS Audit is responsible for auditing the implementation of this policy.

### Risk Assessment Policy

**2.26.1 Overview**

Information risk assessment is an integral part of risk management process designed to provide appropriate levels of security for information systems. It provides an objective, technical evaluation of the likelihood of unacceptable impacts to the XXXX’s information and information assets. Information security risk assessments are part of sound security practice and are key requirements for the Information Security Management and Service Management Systems.

**2.26.2 Purpose**

The purpose of this policy is to describe how the information security risk assessment is managed. This includes the severity of the risk and how it is reported; including the identification of key information assets and their associated risk.

The risk assessment and treatment actions is reviewed on a minimum of an annual basis. The status of risks and, where appropriate, treatment activities will be maintained by Information Security and Operational Risk Management departments.

**Criteria for performing Information Security Risk Assessments**

The following are the circumstances in which a risk assessment should be performed:

* A comprehensive risk assessment covering all information assets as part of the initial implementation of the Information Security Management System (ISMS)
* Updates to the comprehensive risk assessment as part of the management review process
* As part of projects that involve significant change to XXXX or the ISMS
* As part of the IT change management process during the assessment of whether proposed changes would be approved and implemented
* On major change affecting the organization which may invalidate the conclusions from previous risk assessments conducted.
  + 1. **Policy Details**

The tool utilised for conducting the Risk Assessment is the Vigilant Software Risk Solution. The risk assessment would be conducted in two ways:

* **Asset-based Risk Assessment**: Asset-based risk assessments focus on the risks facing individual assets in order to control them.
* **Scenario-based Risk Assessment**: Scenario-based risk assessments look at the risks facing the organization’s information more generally and assess the necessary controls based on those risks.

The following steps are followed during a Risk Assessment process:

1. Identify the Name of the Asset/Service
2. Identify Owner of the Asset/Service
3. Specific type of Asset/Service.
4. The security classification of the information held by the asset
5. Specific identification of the assets.
6. The physical or logical location of the asset
7. The appropriate legal, regulatory and contractual obligations for each asset.
8. The risk to the asset is then assigned a score and calculated.
9. The treatment plan is identified as to how the risk of compromise of the asset/service is to be implemented.
10. The Risk Assessment will be conducted on an annual basis, or when there is a significant change or incident in the XXXX.

**Asset-Based Risk Assessment**

1. View the assessment by ‘owner’
2. Create asset owners
3. Select an asset owner
4. Create asset for asset owner
5. Select risks to the asset
6. Define controls to reduce the likelihood and impact of the risk
7. Repeat from 3 until all assets are made for that asset owner
8. Repeat from 2 for all asset owners

**Scenario-Based Risk Assessment**

1. View the assessment by ‘scenario’
2. Create risk owners
3. Select a risk owner
4. Define a risk for the risk owner
5. Define controls to reduce the likelihood and impact of the risk
6. Repeat from 3 until all risks are made for that risk owner
7. Repeat from 2 for all risk owners

**Risk Acceptance Criteria**

The criteria for acceptance of risk within XXXX shall include:

* When risk value is lower than the acceptance threshold, the risk shall be accepted
* When risk value is higher than the threshold, the risk shall be treated and if after treatment, the likelihood of the occurrence can be reduced or may remain same if controls implemented are not robust enough as certified by Top Management

**2.26.4 DEFINING AND SCORING RISKS**

The impact to the loss of confidentiality, integrity, availability (CIA) is assessed as it relates to the defined asset/service. For each asset/service you have defined, you need to assign risks or scenarios.

The impact to the loss of confidentiality, integrity, availability (CIA) is:

* Assessed and defined in terms of the applicability and compromise it represents (to confidentiality, integrity and/or availability)
* The impact it could result in and the likelihood of the risk coming to pass for individual Assets.

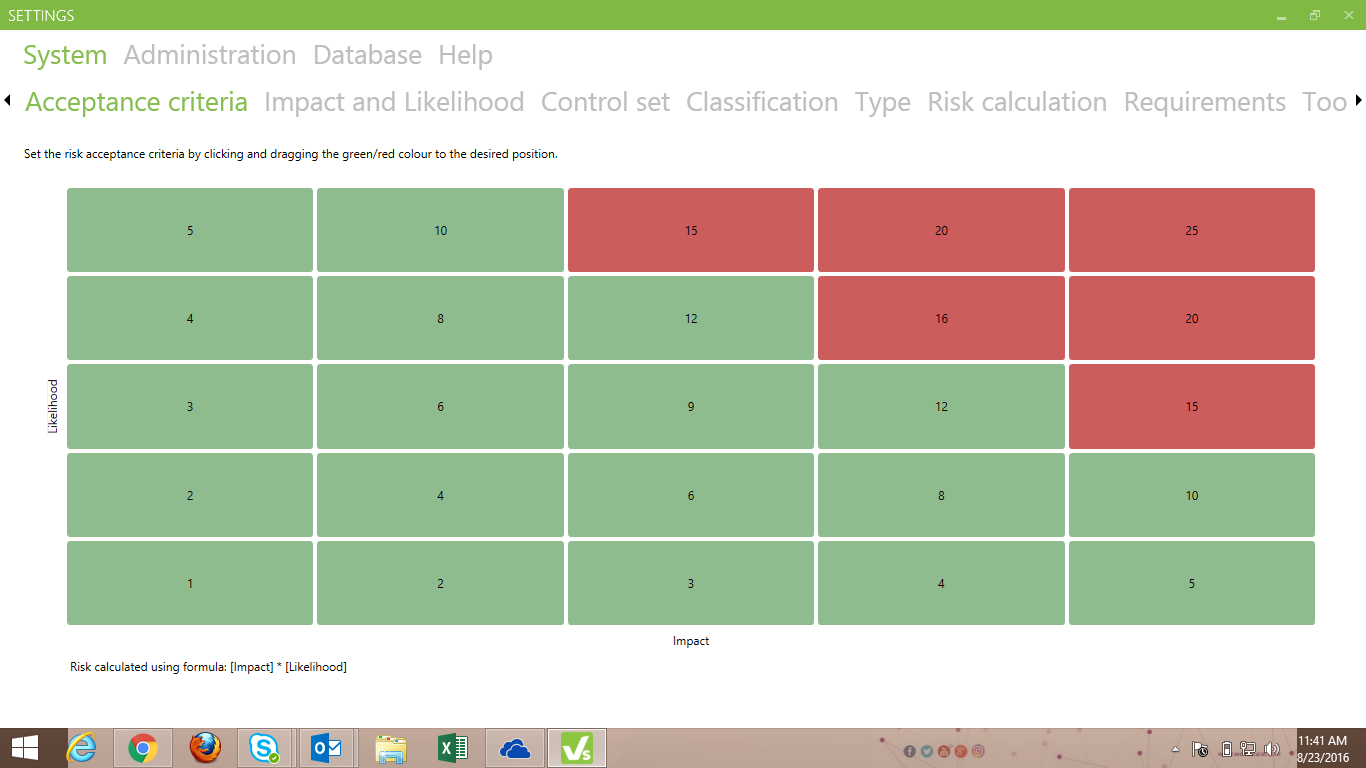
**Likelihood input scales**

* 1 – Rare (Once in 10 years or more)
* 2 – Unlikely (Once in 5 years)
* 3 – Possible (Annually)
* 4 – Likely (Once in 3 months)
* 5 – Expected (Monthly)

**Impact input scales**

* 1 – Insignificant
* 2 – Minor
* 3 – Moderate
* 4 – High
* 5 – Massive

**CALCULATING THE RISK**



* The above diagram details the risk acceptance threshold and the risk assessment formula.
* The risk is calculated using the formula: **[IMPACT] X [LIKELIHOOD]**
* Risk scores that are lower or equals **12** (green) are generally accepted, Risk scores greater than **12** (Red) need mitigation.

**2.26.5 RISK RESPONSE OPTIONS**

* + - 1. **Treat**

Treating the risk means that the organisation will take measures to reduce or eliminate the risk’s impact and/or likelihood. This is handled through the application of controls.

* + - 1. **Tolerate**

This involves the informed decision to accept a particular risk. This may occur with or without treating the risk. For instance, some risks represent such a low impact and/or likelihood that treating the risk does not represent a good return on the necessary investment.

* + - 1. **Transfer**

Some risks can be transferred to other parties, such as through insurance, outsourcing, and so on.

* + - 1. **Terminate**

Terminating a risk means that the risk is too great to permit, but treating it is too expensive or difficult. In these instances, the organisation chooses to find a way to completely avoid the risk itself, such as through the elimination of the asset, restructuring information infrastructure, and so on.

**2.26.6 RISK ASSESSMENT REPORT**

The Risk Assessment report is generated from the VsRisk Solution. This includes the detailed treatment plan for identified assets and services. For each identified treatment the risk decision of Treat, Tolerate, Transfer or Terminate is identified. Acceptance of these risks does not preclude risk treatment activities being carried out.

**2.26.7 RESPONSIBILITIES**

|  |  |
| --- | --- |
| **Role** | **Description** |
| Operational Risk Management | * Review all services/assets on an annual basis * Verify within the Management Review Process * Scoring all risks |
| Chief Information Security Officer | * Review all services/assets on an annual basis * Review all Risk Assessment Reports |
| Information Security Forum | * Review all Risk Assessment Reports * Assign responsibilities to enact the Treatment Plan |
| Designated Owners | * Enact Treatment Plan * Inform Management Representative of actions taken |

### Media Transportation Policy

**2.27.1 Purpose**

This policy sets out the process to be followed for transportation of media on tapes containing data relevant to XXXX.

* + 1. **Policy Details**
* Sensitive data located on information system resources or electronic media must be protected against theft and unauthorized access.
* Sensitive data must be consistently protected and managed through its life cycle, from origination to destruction.
* Information system resources and electronic media for which this policy applies include, but are not limited to, computers (servers, desktops and portable computing devices), backup tapes, portable hard drives and USB storage devices with stored sensitive data.
* Sensitive data in transport is encrypted when warranted/feasible
* An exact copy of sensitive data is maintained in case of loss or damage
* The backup tape register records the following information on tapes removed to archive:
  + What tape was removed to be transported
  + When it was transported
  + Who handled it during transport
  + When it arrived at its final destination
  + Condition upon arrival
* All media sent outside the facility are to be transported in a secure manner.
* The media would be transported to the offsite storage site, the vault warehouse, by at least two appointed staff members in Information Technology and Internal Control Departments.
  + 1. **Responsibilities**
* IT Infrastructure and DBA team will be responsible for understanding and complying with this policy.
* Head IT shall be responsible for implementing this policy.
* Head, IT & Digital Compliance is responsible for ensuring compliance with this policy
* Internal Audit – IS Audit is responsible for auditing the implementation of this policy.

### Mobile Device Policy

**2.28.1 Introduction**

XXXX is committed to and encourages a collaborative environment using mobile devices to facilitate business interaction among customers, suppliers, departments and employees. However, there is an inherent risk in utilizing mobile devices due to the ease with which these items can become lost or stolen.

**2.28.2 Purpose**

The purpose of this policy is to:

* Define standards, procedures, and restrictions for users who have legitimate business requirements to use a private or XXXX’s provided mobile device that can access the XXXX’s information and information resources.
* Clearly state the requirements necessary to mitigate this risk and to protect XXXX’s or personal sensitive information stored on mobile devices.

**2.28.3 Scope**

This policy is applicable to every user, personnel that is granted access/privileges on the company’s premises, information and information systems; these include permanent staff, temporary/contract staff, consultants, vendors and other third parties. Breach of this policy may warrant disciplinary measures, up to and including termination of employment/contract.

This Policy applies to, but is not limited to, all mobile devices and accompanying media that can potentially hold the XXXX’s information, for example: -

* Laptops
* Tablets/Notebooks/PDAs
* Mobile Phones and Smart Phones
* Portable storage such as removable hard drives, USB memory sticks and data cards
* Portable audio visual equipment including data projectors, cameras etc.
  + 1. **Policy Details**
* The XXXX reserves the right to refuse, by physical and non-physical means to allow access to devices or software where it considers that there is a security or other risk to its information or information facilities.
* The XXXX reserves the right to request access to inspect, or delete the XXXX’s information held on a Personally Owned Mobile Device to the extent permitted by law and for legitimate business purposes. Every effort will be made to ensure that the XXXX does not access the private information of the individual.

Where an employee has any mobile device having the XXXX’s information, they shall at all times:

* Ensure the security and safety of the device; such device shall be password protected where the feature exists
* Ensure the device is connected to the network (if appropriate) on a regular basis in order to run any updates to system and anti-virus software;
* Ensure that removable storage is not utilised;
* Where it is practicable, ensure that no personal information is retained on the mobile device, such as personal accounts and passwords;
* It is the user’s responsibility to report any instances of possible viruses, Trojans or phishing attempts.
* No information which has been classified as confidential shall be retained on any mobile device;
* Information classified as Confidential if stored on a portable storage media shall be encrypted where feasible
* The information on the mobile device shall be immediately and permanently erased once the data on them are no longer required
* Ensure that wherever possible, device is placed in stable and secure locations to minimise the possibility of damage from tripping or dropping.
* Should a mobile device be lost or stolen, the Information Security Incident Policy is to be followed and any authorities contacted as is deemed necessary.
  + 1. **Responsibilities**
* All staff will be responsible for understanding and complying with this policy.
* Head, IT shall be responsible for implementing this policy.
* Head, Information Security is responsible for ensuring compliance with this policy
* Internal Audit – IS Audit is responsible for auditing the implementation of this policy.

1. **Communications Policy**

**2.29.1 Purpose**

This policy simply describes the modes of communication of the ISO Management System for XXXX to satisfy and comply with the requirements of the ISO 27001:2013 Standard. It outlines communication lines with key inputs and outputs of the ISO Management System communication.

* + 1. **Policy Details**

**ISO Internal Communications**

All ISO related and Information Security matters should be communicated using the following methods detailed in the table below:

* Roles: Who is responsible for communicating
* What: Outputs that are to be communicated
* When: Frequency of communication
* Who: Intended audience for the communication
* Method: How information is communicated

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Roles | What | When | Who | Method |
| Top Management | Objectives | Annually | All Staff | Policy Statement |
| Management Review | Annually | Information Security Forum | Management Review Minutes |
| Information Security Steering Committee(ISF) | Management Review | Quarterly | Top Management | Management Review Minutes |
| ISO Sponsor | All ISO matters | Ongoing Basis | Top Management /  ISF | Email  Phone  Verbal  Reports |
| Management Representatives | Action and Treatment Plans | Bi-annually | ISF | Reports |
| External Audits | Annually | ISF | Reports |
| Risk Assessments | Annually | ISF | Reports |
| Internal Audits | Annually | Certification Body/  ISF | Reports |
| Policies | Annually/Upon request | All Staff/  Certification Body/  Designated Interested Parties | Intranet  Email  Banners |
| Processes | Annually/Upon request | All Staff/  Certification Body/  Designated Interested Parties | Intranet |
| Business Continuity Plans (BCP) | Annually/Upon Changes | BCP Teams | Emails  Meetings |
| ISO Champions | ISO Awareness | Ongoing | All Staff | Departmental Meetings  Awareness Session |
| ISO Internal Auditors | ISO Audit Plan | Annually | Management Reps | ISO Audit Plan |
| ISO Audit Results | Annually | Management Reps | ISO Internal Audit Reports |
| All Employees | Incidents | Ongoing | Head of Department/  Incident Response Team | Email  Memos  Helpdesk |
| Events | Ongoing | Head of Department/  Incident Response Team | Email  Helpdesk |
| Non-conformances | Ongoing | Head of Department/  Incident Response Team | Email  Helpdesk |
| Improvements | Ongoing | Head of Department/  Management Reps | Email  Meetings |

**External Communications**

* All ISO documentation are classified as per the Information Classification Policy.
* Only documents that are classified as Public Information may be distributed to designated interested parties.
* Should any interested party request access to other classifications of documents they are to be invited to premises and supervised whilst viewing these documents.
* No copies are allowed to be transferred to external parties. Alternatively redacted and therefore declassified versions of documents may be distributed to external parties.
  + 1. **Responsibilities**
* All staff will be responsible for understanding and complying with this policy.
* ISO Management Representative shall be responsible for implementing this policy.
* Head, Information Security is responsible for ensuring compliance with this policy
* Internal Audit – IS Audit is responsible for auditing the implementation of this policy.

### Software Management Policy

**2.30.1 Purpose**

To establish guidelines and procedures for managing software on the XXXX’s network

* + 1. **Policy Details**
* All users must ensure that only software developed, or acquired, through approved procedures must be installed on computers.
* As part of the requirements gathering exercise in the design phase of any software deployment (purchased or developed in-house), the XXXX’s security policy shall serve as a benchmark to ensure the XXXX’s information security requirements are met by the new solution. This requirement shall guide the software selection/development process.
* Security requirements shall be incorporated into the early stages of Software Development Life Cycle. Hence, a meeting of all stakeholders – IT & Digital Compliance, Information Security, IS Audit, Business & Operation Risk, IT and the Business must be conveyed before any development or acquisition can commence.
* A Risk Assessment shall be conducted by an assessment team comprising representatives from Business & Operational Risk Management, IS Audit, Information Security, IT & Digital Compliance & Compliance on all critical business applications (in-house developed and vendor solutions) and Operating systems prior to deployment in a live environment (production). Business applications are deemed critical if they interface with the XXXX’s core XXXXing application or may result in a material loss to the XXXX in the event of security compromise, system downtime impacting business operations or any operational issue that may adversely affect the XXXX’s operations. Business applications are also deemed critical if its downtime will cause regulatory sanctions to the XXXX.
* The risk assessment shall be documented and filed as part of the pre Go-Live system requirements for audit purposes. The outcome of the Risk Assessment shall be a report detailing all the risks, mitigating controls, risk rating/ranking and remedial action plans for identified gaps.
* A certification/sign-off shall be provided by the Risk Assessment team, as part of the pre Go-Live tests, prior to system cut-over to the production environment. The certification/sign-off is an acceptance by the team that the inherent risks of the business application have been satisfactorily mitigated to the extent that the XXXX will not be exposed to any significant risks upon deployment.
* All software developed in-house must be stored in a software library and in custody of the software librarian for safekeeping.
* All software developed in-house automatically becomes the XXXX’s intellectual property. Such software, or a part of it, must not be re-used by the development team for personal purpose or even for a competition when the staff has exited the XXXX.
* All requests for new applications systems or software enhancements must be presented to senior management with a Business Case with the business requirement presented in a user requirement specification document.
* The XXXX shall avoid the selection of business critical software which, in the opinion of management has not been adequately proven by the early adopters of the system. Selection must also incorporate the criteria upon which the selection will be made. Such criteria must receive the approval of senior management.
* Where applicable, XXXX shall seek for an escrow agreement with the vendor for all critical business application before purchasing of the software.
* All software packages to be implemented on the XXXX IT Infrastructure must be compatible with the XXXX’s operating system and platform
* All implemented software packages must have a maximum idle session timeout of five (5) minutes.
* All applications must validate input properly and restrictively, allowing only those types of input that are known to be correct.
* All applications must execute proper error handling so that errors will not provide detailed system information, deny service, impair security mechanisms, or crash the system.
* Applications that handle some form of financial transactions must have the “Maker-Checker” controls capabilities. The application must provide automated review of authorizations.
* Implementation of application logs to the extent practical, given the limitations of certain systems to store large amounts of log data. When logging access to XXXX’s data, store logs of all users and times of access.
* To comply with legislation and to ensure ongoing vendor support, the terms and conditions of all End User License Agreement (EULA) are to be strictly adhered to
* Patches to resolve software bugs may only be applied where verified as necessary and with IT management authorization. Patches must be from a reputable source and are to be thoroughly tested before use
* Upgrade to software must be properly tested by qualified personnel before they are used in a live environment
* Software developed in-house shall be certified by Information Security and IT & Digital Compliance controls function in the XXXX prior to deployment.
  + 1. **Responsibilities**
* All employees of XXXX are required to understand this policy
* Head, IT is responsible for enforcing this policy
* Head, Information Security is responsible for ensuring compliance with this policy
* Internal Audit – IS Audit is responsible for auditing the implementation of this policy

**2.30.4 Checklist for Information Security Requirements for Software Selection/Developments**

| **S/N** | **Requirements/Best Practice** | **Remark** |
| --- | --- | --- |
| 1 | Ensure that Application validates Input properly and restrictively, allowing those kind of input that are known to be correct. Examples include, but not limited to, such possibilities as cross-site scripting., buffer overflow errors, and injection flaws | Required |
| 2 | Ensure applications executes proper error handling so that errors will not provide detailed system information, deny service, impair security mechanisms, or crash the system | Required |
| 3 | Ensure applications processing data properly authenticate users through central authentication systems, specifically, the Active Directory. Where the application cannot authenticate users via AD, the application must ensure that:   1. Each user is assigned a unique username 2. Each user must be forced to change initial password at first login 3. Password must expire after 30 days of usage so that users can periodically change passwords 4. Passwords must have 8 or more character containing alphanumeric and special characters to ensure strong password 5. Password should not be reused until after 6 changes | Required |
| 4 | Applications must ensure maximum idle session timeout of 5 minutes | Required |
| 5 | Applications that handle some form of financial transactions must have the ‘Maker-Checker’ controls capabilities. The application must provide automated review of authorizations. | Required |
| 6 | Services or application running on systems manipulating data should implement secure (i.e. encrypted) communications as required by Confidentiality, and Integrity needs. The application must be able to encrypt users’ password and audit trails. | Required |
| 7 | It must be able to implement the use of application logs to the extent practicable, given the limitations of certain systems to store large amounts of log data. When logging access to XXXX’s data, store logs of all users and times of access. | Required |
| 8 | Implement and maintain a change management process for changes to existing software applications. Conduct code-level security reviews with professionally trained peers for all new or significantly modified applications; particularly. Those that affect the collection, use, and/or display of confidential data, documenting the actions that were taken. | Required |
| 9 | Certificate and assurance of ISO 8085 communication standard must be obtained for all off-the-shelf applications | Required |

### Hardware Management

**2.31.1 Purpose**

* To establish guidelines and procedures for managing the use of desktop and laptop computers on the XXXX network
* To establish guidelines and procedures for managing security of devices
  + 1. **Policy Details**
* The use of Laptop computers shall be limited to staff based on category, department and job function as defined by user categorization in the IT policy.
* Only categories of staff (Assistant Manager and above) shall have access to laptop computers (except where job function requires otherwise). On a “need only” basis shall laptops be assigned to individuals whose job functions / units require the use of laptops. Such exemptions shall be approved by the Head of HR, Chief Information Officer or Divisional Head, Operations.
* Laptops assigned to a unit / department remain the property of XXXX.
* On staff disengagement, these systems shall be returned to the respective unit as part of the HR disengagement requirements.
* All laptop and desktop computers which are inactive for a period exceeding 3 minutes shall be automatically locked with a screen or keyboard-locking device
* System Administrator shall ensure users are unable to copy data from Laptop and desktop computers unto an external hard drive / flash stick/ computer diskettes or any other external backup device.
* Desktops and Laptops used for XXXX work purposes shall not be used for gaming and video streaming. Only approved applications and images of the XXXX shall be displayed on systems. For the Laptop policy, refer to the XXXX IT Policy - “Computer and Internet Usage Policy”
* All diskettes, tapes, CD-ROMs and other computer readable media shall be secured to prevent theft, loss or corruption; using centrally managed safe storage facilities when appropriate
* All laptop or desktop computers must be secured with a reliable login password
* Desktop computers left unattended for a long period shall be switched off or locked with a screen or keyboard-locking device
* All security incidents (virus, hacking, theft, etc.) must be reported by the user and any suspected weaknesses or software malfunction reported immediately to the IT Help desk
* Only personnel authorized to install or modify software shall use removable media to transfer data to / from the XXXX network. Any other persons shall require specific authorization from the Head, IT
  + 1. **Responsibilities**
* All staff will be responsible for understanding and complying with this policy.
* Head IT shall be responsible for implementing this policy.
* Head, Information Security is responsible for ensuring compliance with this policy
* Internal Audit – IS Audit is responsible for auditing the implementation of this policy.

### Access to Operating System Software

**2.32.1 Purpose**

To establish guidelines and procedures for managing access to operating systems

**2.32.2 Policy Details**

* Access to Operating system commands shall be restricted to those persons who are authorized to perform systems administration / management functions. Such access must be operated under dual control requiring the specific approval of the Group Head, IT
* Upon installation of operating systems all default passwords for privileged default accounts must be changed.
* Access to the Root account on UNIX shall not be used for routine activities by the system administrator. Individual user accounts tied to specific users shall be created for daily admin tasks and user activities.
* All systems, from PCs to Large Servers, shall be hardened to remove all unnecessary development tools and utilities prior to delivery to end users
  + 1. **Responsibilities**
* IT support staff are expected to understand and comply with this policy
* Head, IT is responsible for enforcing this policy
* Head, Information Security is responsible for enforcing compliance to this policy
* IS-Audit is responsible for auditing the implementation of this policy.

### Data Governance Policy

**2.33.1 Introduction**

Data Governance is the specification of decision rights and an accountability framework to encourage desirable behaviour in the valuation, creation, storage, use, archiving and deletion of information. It includes the processes, roles, standards and metrics that ensure the effective and efficient use of information in enabling an organization to achieve its goals.

Information is a strategic asset of XXXX. and the appropriate governance for management and use of information is critical to the XXXX’s operations. Inappropriate governance can result in inefficiencies and exposes the XXXX to unwanted risk. A consistent, repeatable, and sustainable approach to data governance is therefore necessary in order to protect the security and integrity of the XXXX’s information assets.

**2.33.2 Purpose**

The purpose of the Data Governance Policy is to:

* Establish fundamental principles governing the management and use of data and information including, but not limited to, the creation or acquisition, privacy and security, integrity and quality of data and information
* Establish clear lines of accountability and decision rights through the definition of roles and responsibilities related to data management
* Develop best practices for effective data management and protection;
* Ensure that the XXXX complies with applicable laws, regulations, and standards of Information.

**2.33.3 Scope**

This policy applies and is of importance to all employees of the XXXX, including temporary Staff, external partners/vendors and contractor personnel and other third parties. Conformance to this Data Governance Policy is therefore required from the moment an employee joins XXXX until the moment he/she leaves.

The scope of this Data Governance Policy includes, but is not limited to:

* All information processed by the XXXX in pursuit of all its operational activities, regardless of whether it is processed electronically or in paper form, including but not limited to:
  + Customer information
  + Operational plans, documents and records
  + Employee records
* All information processing facilities used in support of the XXXX’s operational activities to store, process and transmit Information
* All external organisations that provide services to the XXXX in respect of information processing facilities
* Sensitive information which are subject to privacy considerations or has been classified as confidential and are therefore subject to protection from public access or inappropriate disclosure.

Violations of this policy will be documented and can lead to revocation of system privileges and/or disciplinary action up to and including termination.

**2.33.4 Objectives**

The objective of the Data Governance Policy is to:

* Define, approve, and communicate Information strategies, policies, standards, architecture, procedures, and metrics.
* Support a culture of responsible data usage for informed and actionable decision making
* Increase the XXXX’s transparency and accountability to external stakeholders and the public by promoting access to relevant information.
* Track and enforce conformance to Information policies, standards, architecture, and procedures.
* Sponsor, track, and oversee the delivery of data management projects and services.
* Understand and promote the value of information assets.

**2.33.5 Policy Details**

* XXXX., rather than any user or department, is the owner of all data/Information.
* The XXXX’s Data will be managed through defined governance guidelines, standards, policies and procedures
* A Data Steering Committee, in the form of the Information Security Steering Committeeis responsible for the overall management of the XXXX’s data governance.
* XXXX’s Data must be safeguarded and protected according to approved security, privacy and compliance guidelines, laws, and regulations.
* All Data Owners has the responsibility for the management of data assigned within their portfolio. Data Owners are responsible for ensuring effective local protocols are in place to guide the appropriate use of data.
* Every data source must have a Data Owner who is responsible for the quality and integrity, implementation and enforcement of data management within their department.
* Access to, and use of, the XXXX’s data will generally be administered by the appropriate Data Owner.
* The Data/Technology Steward, having determined the category of the XXXX’s data as confidential, will approve access based on appropriateness of the User’s role and the intended use. Where necessary, approval from the Data Governance Head may be required prior to authorisation of access.
* Data quality standards shall be defined, published, communicated, managed, and applied according to the reliability and risk levels established by the Data Steward.
* Maintenance of XXXX’s Data to ensure appropriate backup, retention, destruction, identification, etc. will be defined by appropriate Data owners and the Technology Steward.
* All Users must ensure appropriate procedures are followed to uphold the quality and integrity of the data they access.
* All records must be kept up-to-date throughout every stage of the workflow and in an auditable and traceable manner.
* Extraction, manipulation and reporting of data must be done only to perform the XXXX’s Operations
* Personal use of XXXX’s data, including derived data, in any format and at any location, is prohibited.
* Where appropriate, before any data (other than publically available data) is used or shared outside the XXXX, verification with the Data Steward is required to ensure the quality, integrity and security of data will not be compromised.
* Data stored in an electronic format must be protected by appropriate electronic safeguards and/or physical access controls that restrict access only to authorised user(s). Similarly, data in hard copy format must also be stored in a manner that will restrict access only to authorised user(s).
* Appropriate data security measures (see Information Classification and Control Policy) must be adhered to at all times to assure the safety, quality and integrity of XXXX’s data.
* Data shall be retained and disposed of in an appropriate manner in accordance with the XXXX’s Information Disposal policy and Data Retention Policy.
  + 1. **Responsibilities**

|  |  |  |
| --- | --- | --- |
| **ROLE** | **RESPONSIBILITY** |  |
| **Data Steering Committee** | The Steering Committee will provide strategic direction to the Data Governance Organization, and oversee policy, issues and communication. | Information Security Forum |
| **Data Governance Sponsor** | * The Executive Sponsor provides overall guidance to the organization. | * ED |
| **Data Governance Head** | * The Data Governance Head provides tactical and strategic guidance to the XXXX’s data and information | * CISO |
| **Data Owners** | * The Data Owners are the decision makers for establishing data quality requirements. Responsibilities include:   + Owning the implementation and ongoing management of data quality improvements   + Establishing data quality requirements (timeliness, accuracy, completeness, accessibility)   + Determining and approving access and re-use of data   + Understanding legal/compliance/regulatory issues impacting data   + Setting priorities and sponsoring projects for all work related to the maintenance and processing of the data   + Approving all governance matters impacting the processing of data | * HODs |
| **Data**  **Steward** | * The Data Steward manage the process to maintain the data for the owner. Responsibilities include:   + Assisting with issue tracking, escalation and resolution   + Documenting data definitions (Business Glossary)   + Proposing changes and/or improvements to the Data Owner to improve efficiency or resolve issues   + Acting as proxy for Data Owner on projects, initiatives and operational functions | * Head, BPR |
| **Technology Steward** | * The Technology Stewards manage the technology to maintain the data. Responsibilities include:   + Developing and maintaining the applications that automate data processes   + Providing system data documentation (metadata, dictionaries, lineage)   + Coordinating all IT activities to maintain and develop the technology platform   + Ensuring the technology is appropriate to meet data quality requirements   + Ensuring data security, backup, and archiving requirements are being met   + Proposing changes for upgrades/improvements/risk mitigation in the technology environment   + Ensuring that the technology is aligned with Enterprise Architecture standards | * Head, IT |
| **Business Representatives** | * The Business Representatives reside within the business groups and serve as the data authority for their business area. Responsibilities include:   + Ensuring data quality through fit-for-purpose requirements which are developed by the data owners   + Identifying and prioritizing for improvement key systems or processes   + Supporting the firm’s data quality efforts through accountability to, and close interaction with, the Core Data Governance Team | * Departmental ISO Champions |
| **Data Consumers** | Data Consumers, also known as users, are employees, vendors and/or third parties of the  XXXX who access XXXX’s Data in performance of their assigned duties. | * All Users |

### Social Media Policy

**2.34.1 Introduction**

XXXX. is committed to making the best use of all available technology and innovation to improve the way we do business. This includes using all reasonable and cost-effective means to improve the way we communicate, reach out and interact with our customers. Social media' is the term commonly given to web-based tools which allow users to interact with each other in some way – by sharing information, opinions, knowledge and interests online. As the name implies, social media involves the building of online communities or networks to encourage participation and engagement.

These platforms open up many new and exciting opportunities. However, the practical application of such technology by the XXXX is continually developing and there are many potential issues to consider – both as users and as a XXXX.

**2.34.2 Purpose**

The purpose of the Social Media Policy is to:

* Provide users with information concerning the use of, or the development of, any social media application
* Help users get the best out of the tools available whilst maintaining a safe professional environment and protecting themselves, as well as the XXXX.

**2.34.3 Scope**

This document applies and is of importance to all employees of the XXXX, including temporary Staff, external partners/vendors and contractor personnel and other third parties. Conformance to this policy is therefore required from the moment an employee joins XXXX until the moment he/she leaves.

Serious breaches of these guidelines, for example incidents of bullying of colleagues on social media or social media activity causing serious damage to the XXXX, will be documented and can lead to revocation of system privileges and/or disciplinary action up to and including termination.

**2.34.4 Policy Details**

* Employees must adhere to the XXXX’s Code of Conduct, Employee Handbook, and other XXXX’s policies when using social media in reference to XXXX.
* Employees may contribute to the XXXX's social media activities in accordance with the standards defined by the Brand and Marketing Department.
* Employees are not to publish, post or release any information that is considered confidential or not public. If there are questions about what is considered confidential, employees should check with the Information Security or Brand and Marketing Department and/or line Manager.
* The XXXX understands that employees may wish to use their own computers or devices, such as laptops, tablets and mobile telephones, to access social media websites while they are at work. Such use should nonetheless be in accordance with these guidelines.
* Employees must be aware at all times that, while contributing to the XXXX's social media activities, they are representing the XXXX. Staff who use social media as part of their job must adhere to the following safeguards.
* Employees should use the same safeguards as they would with any other form of communication about the XXXX in the public sphere. Such safeguards include:
* making sure that the communication has a purpose and a benefit for the XXXX;
* obtaining permission from the authorities before embarking on a public campaign using social media;
* getting the Brand and Marketing department to check the content before it is published.
* Any communications that employees make in a professional capacity through social media must not breach confidentiality, do anything that could be considered discriminatory against, bullying or harassment of any individual, bring the XXXX into disrepute or breach copyright.
* Social media use shouldn't interfere with employee’s responsibilities. The XXXX’s computer systems are to be used for business purposes only. The use of social media networks for business purposes is allowed but personal use of social media is discouraged and could result in disciplinary action.
* The XXXX reserves the right to monitor users’ internet usage in accordance with the Information Security Policy and Internet Usage Policy
* The XXXX reserves the right to monitor and, as defined within the Information Security Policy and associated IS policies to retain information that it has gathered on employees' use of the internet.
* Access to particular social media websites may be withdrawn in any case of misuse.
* The XXXX recognises that users make use of social media in a personal capacity. While they are not acting on behalf of the XXXX, users must be aware that they can damage the XXXX if they are recognised as being one of our employees.
* Where a user releases information through Social Media that may be considered as a Public Interest Disclosure (Whistle Blowing), the XXXX’s whistleblowing policy, must be initiated in the first instance before any further action is taken.
  + 1. **Responsibilities**

1. All users are required to understand this policy and put into action.
2. Head, Brand and Marketing and Head, IT is responsible for implementing this policy.
3. Head, Information Security is expected to ensure adherence to this policy
4. Internal Audit – IS Audit is responsible for auditing the implementation of this policy.

### Wi-Fi Acceptable Use Policy

**2.35.1 Introduction**

The wireless network is intended as a supplement to the wired network and for use with portable electronic devices. The Wireless Network (named as Wi-Fi) is provided to facilitate and support official activities required in the XXXX. This document establishes specific guidelines for the use of the Wi-Fi network resources at XXXX.

**2.35.2 Purpose**

The purpose of this policy is to protect the XXXX’s information and information assets from unauthorized use and/or malicious attack that could result in loss of information, damage to critical applications, or damage to our public image.

**2.35.3 Scope**

This policy is applicable to every user that is granted access/privileges on the company’s wireless network; these include permanent staff, temporary/contract staff, consultants, vendors and other third parties. No one is permitted to bypass the security mechanisms provided by the company’s systems or infrastructure for any reason. Breach of this policy may warrant disciplinary measures, up to and including termination of employment/contract.

All users must understand and adopt use of this policy and are responsible for ensuring the safety and security of the XXXX. Violations of this policy will be documented and can lead to revocation of system privileges and/or disciplinary action up to and including termination.

**2.35.4 Policy Details**

* Only authorized users will be allowed to have access to the service and must only be used by the person for whom it was originally intended.
* All users who are registered on the wireless service shall be governed by this Policy and the Internet usage Policy
* Wireless Access will be provided by default for Executive Management on all their devices
* Access Points will be made available in all meeting rooms within the Head Office.
* Wireless connectivity is a supplement to the Wired connection and approval for wireless access will be given on a needs basis.
* All wireless devices on the XXXX's network must be approved and centrally managed by the XXXX’s Information Security department.
* It is the user’s responsibility to ensure the device used to access this service has an appropriate level of security and protection against malicious means.
* It is not acceptable to use the wireless connection for any (but not limited to) the following:
* the creation, transmission, downloading or printing of any offensive, obscene, pornographic or indecent images, data or other material, or any data capable of being resolved into pornographic or indecent images or material
* the creation, display or transmission of material which is designed or likely to cause annoyance, inconvenience, unnecessary anxiety, threats or the promotion of violence;
* the creation, display, downloading or transmission of defamatory or discriminatory material especially anything likely to promote religious or racial hatred
* the transmission or downloading of anything other than copyright free material
* the transmission of unsolicited commercial or advertising material
* deliberate unauthorised access (i.e. “Hacking") to any facilities or services accessible on the network
* deliberate activities such as attempting to introduce a computer virus, attempting to corrupt or destroy data, disrupting the work of other users
* The Information Security department will continuously conduct sweeps of the wireless network to ensure there are no rogue access points present.
* The Information Security department reserves the right to turn off without notice any access point connected to the network that it feels puts the XXXX's systems, data, and users at risk.
* Access to the wireless network shall be terminated upon resignation or termination.
* Any breach of these terms and condition of use, permission to use this service will be terminated.
  + 1. **Responsibilities**
* All users are required to understand and comply with this policy at all times.
* Information Security Manager is responsible for implementing this policy
* CISO is responsible for ensuring adherence to this policy
* Internal Audit – IS Audit is responsible for auditing the implementation of this policy.

### CCTV Policy

**2.36.1 Introduction**

XXXX. is committed to enhancing the quality and security of its business environment, practices of safety and security with technology. A critical component of a comprehensive security plan is the utilization of a security and safety camera system. The surveillance of the XXXX’s environment and close public areas is intended to deter crime and assist in protecting the safety and property of XXXX. This policy addresses the XXXX’s safety and security needs while respecting and preserving individual privacy.

**2.36.2 Purpose**

This Policy is established to achieve the following:

* Regulate the use of video surveillance and recording on XXXX’s offices
* Exclusive use of Information obtained through video surveillance for security and law enforcement purposes, which must relate to the protection of customers, staff and the public, or the deterrence or detection of criminal activity, including theft, vandalism, or other property damage.

**2.36.3 Scope**

This policy is applicable to every user, personnel that is granted access/privileges on the company’s premises, information and information systems; these include permanent staff, temporary/contract staff, consultants, vendors and other third parties. Security cameras may be installed in situations and places where the security and safety of either property or persons would be enhanced. Cameras will be limited to uses that do not violate the reasonable expectation of privacy as defined by law. Where appropriate, the cameras may be placed around, inside and outside buildings. No one is permitted to bypass these security mechanisms provided by the company’s systems or infrastructure for any reason. Breach of this policy may warrant disciplinary measures, up to and including termination of employment/contract.

All users must understand and adopt use of this policy and are responsible for ensuring the safety and security of the XXXX. Violations of this policy will be documented and can lead to revocation of system privileges and/or disciplinary action up to and including termination.

**2.36.4 Policy Details**

Video surveillance of the XXXX’s premises will be conducted in a professional, ethical and legal manner, in accordance with the following principles:

* Video surveillance must be conducted in accordance with the laws of Federal Government of Nigeria;
* Video surveillance will be used only where it is demonstrably necessary for the purposes of enhancing the safety of persons, or for the deterrence of theft or destructive acts, such as vandalism.
* Video surveillance will be used only by security officers and information security analyst authorized by the CISO, and only where less intrusive means of deterrence, such as monitoring by Security officers, has been shown to be ineffective or unworkable.
* Appropriate signs and notice of video surveillance must be posted in areas subject to video monitoring;
* Information obtained from the cameras shall be used for safety and security purposes and for law and policy enforcement, including, where appropriate.
* Employees and video service provider(s) will have access to information collected through video surveillance only where necessary in the performance of their duties and in accordance with the provisions of this Policy.
* The recording medium must be handled in a manner that maintains the integrity and security of the recorded information;
* Reception equipment locations and operation shall be limited to visual access of areas where there is no reasonable expectation of privacy. Video surveillance for the purpose of monitoring work areas, social areas, or sensitive areas will only occur in special circumstances, and must be consistent with the policy’s principle purpose, which include the prevention/deterrence of illegal activity and the enhancement of safety;
* When video surveillance footage is being displayed by authorized employees on a video monitor, the monitors will be in a position that cannot be viewed by others.
* The video surveillance system will be subject to periodic audit.
* Authorized and unauthorized Staff are prohibited from using or disseminating information acquired from the XXXX’s security cameras, except for official purposes. All information and/or observations made in the use of security cameras are considered confidential and can only be used by the XXXX’s official and law enforcement purposes.
  + 1. **Responsibilities**
* All users are required to understand and comply with this policy at all times.
* Security Officers, IT & Digital Compliance Officers and Information Security Officers are responsible to operate and monitor the video surveillance system(s) when and as directed.
* The Security Manager is responsible to manage and coordinate maintenance of the video surveillance system(s).
* CISO is responsible for ensuring adherence to this policy
* Internal Audit – IS Audit is responsible for auditing the implementation of this policy and use it as a tool for investigation.

### Bring Your Own Device (BYOD) Policy

**2.37.1 Introduction**

XXXX recognises the benefits that can be attained by allowing users to use their own electronic devices when working, whether that is at home or while travelling. Such devices include laptops, smart phones and tablets, and the practice is commonly known as ‘bring your own device’ or BYOD. The use of such devices to create and process the XXXX’s information and information assets creates issues that need to be addressed, particularly in information security therefore ensuring that as few technical restrictions as reasonably possible are imposed on accessing the XXXX’s provided services on BYOD.

The XXXX must ensure that it remains in control of the data for which it is responsible, regardless of the ownership of the device used to carry out the processing. It must also protect its intellectual property as well as empowering users to ensure that they protect their own personal information.

**2.37.2 Purpose**

The purpose of this policy is to:

* Set guidelines for user’s conduct necessary to protect the privacy, security and integrity of the XXXX’s information and information assets against the risks that can arise when users use their personally owned devices for business purposes.

**2.37.3 Scope**

This policy is applicable to every user, personnel that is granted access/privileges on the company’s premises, information and information systems; these include permanent staff, temporary/contract staff, consultants, vendors and other third parties. Breach of this policy may warrant disciplinary measures, up to and including termination of employment/contract.

This Policy applies to, but is not limited to, all XXXX-owned and personal mobile devices and accompanying media that can potentially hold the XXXX’s information, for example: -

* Laptops
* Tablets/Notebooks/PDAs
* Mobile Phones and Smart Phones
* Portable storage such as removable hard drives, USB memory sticks and data cards
* Portable audio visual equipment including data projectors, cameras etc.

**2.37.4 Policy Details**

* Prior to accessing the XXXX’s information and information resources, all users must present their BYOD devices to the Information Technology department.
* All Users are expected to protect personal devices used for work-related purposes from loss, damage or theft.
* To secure sensitive XXXX information/data, users are required to have “remote-wipe” software installed on their personal devices by the IT department prior to using the devices for work purposes. This software allows the XXXX-related data to be erased remotely in the event the device is lost or stolen. Wiping XXXX data may affect other applications and data. install and configure tracking and/or wiping services, such as Apple’s ‘Find My iPhone app’, Androids ‘Where’s My Droid’ or Windows ‘Find My Phone’, where the device has this feature. •
* remove any XXXX information stored on your device once you have finished with it including deleting copies of attachments to emails, such as documents, spreadsheets and data sets, as soon as you have finished using them. •
* limit the number of emails and other information that you are syncing to your device to the minimum required. •
* Remove all XXXX information from your device and return it to the manufacturers’ settings before you sell, exchange or dispose of your device.
* The XXXX will not be responsible for loss or damage of personal applications or data resulting from the use of XXXX applications or the wiping of XXXX information.
* Upon resignation or termination of employment, or at any time on request, the user may be asked to produce the personal device for inspection. All XXXX’s data on personal devices will be removed by IT upon termination of employment.

All users must take appropriate secure measures under the XXXX’s acceptable use Policy including but not limited to:

* Ensuring that their BYOD device is password protected using the features of the device and that a “strong password,” as defined in the Password Policy, is required to access the XXXX’s network and information
* Ensuring that their BYOD device locks itself with a password or PIN if the device is idle for one minute
* Ensuring that their BYOD device locks itself and must be re-opened by another password or PIN after three failed login attempts
* Not using rooted (Android) or jailbroken (iOS) devices to access the XXXX’s information and network
* Not sharing their BYOD devices with friends, relatives
* Not storing or transmit illicit material or proprietary information belonging to another organisation
* Using their BYOD devices to access only the information authorized to access under the XXXX authentication and authorization procedures;
* Maintain the BYOD device themselves ensuring it is regularly patched and upgraded
* Reporting lost, misplaced or stolen BYOD devices to the IT department within 24 hours
* Paying all costs associated with purchasing and their BYOD device.
* Report any security breach immediately to Information Security Team in accordance with the Information Security Policy
* Authorized users are required to have anti-virus and mobile device management (MDM) software installed on their personal mobile devices.
* Users are expected to exercise the same discretion in using their personal devices as is expected for the use of the XXXX’s devices. The XXXX’s policies pertaining to harassment, discrimination, retaliation, trade secrets, confidential information and ethics applies to the use of personal devices for work-related activities.
* The XXXX has the right, at any time, to monitor and preserve any communications that uses its networks in any way, including data, voice mail, telephone logs, Internet use and network traffic, to determine proper use.
* No user may knowingly disable any network software or system identified as a monitoring tool.
* The use of your own device MUST adhere to the XXXX’s Information Security Policy
* From time to time, the XXXX may require that you install or update XXXX-approved device management software on your own device.
* It is your responsibility to familiarise yourself with the device sufficiently to keep data secure.

The XXXX’s IT department may remotely wipe a user’s BYOD device may be remotely wiped if:

* The device is lost or stolen
* The Information Technology / Information Security department detects a data or policy breach, virus or other threat to the security of the XXXX’s data/information and infrastructure; and/or
* The user’s employment is terminated.

**2.37.5 Responsibilities**

* All users will be responsible for understanding and complying with this policy.
* Head, IT shall be responsible for implementing this policy.
* Head, Information Security is responsible for ensuring compliance with this policy
* Internal Audit – IS Audit is responsible for auditing the implementation of this policy.

### Log Management Policy

## 2.38.1 Introduction

The information held within and managed by the XXXX shall, where possible, be protected against the consequences of breaches of confidentiality, failures of integrity or interruptions to its availability to authorised users. Monitoring and logging of the XXXX’s information systems will be carried out in order to help protect the safety of the XXXX, and in order to preserve the confidentiality, integrity and availability of the data held upon the XXXX’s information systems. It will also assist in capacity planning by analysing usage patterns and warning before systems reach capacity.

## 2.38.2 Purpose

* To address the requirements for safeguarding the confidentiality, integrity, and availability of XXXX. information assets through auditing, logging, and monitoring activities.
* To verify compliance with access controls and administrative and other safeguards developed and implemented to prevent/limit inappropriate access to data.
* To ensure that routine and random audits are utilized as oversight tools for recording and examining access to information
* To detect authorized and unauthorized information processing activities

## 2.38.3 Scope

This document applies and is of importance to all employees of the XXXX, including temporary Staff, external partners/vendors and contractor personnel and other third parties. Conformance to this policy is therefore required from the moment an employee joins XXXX until the moment he/she leaves.

Breaches of these guidelines will be documented and can lead to revocation of system privileges and/or disciplinary action up to and including termination.

## 2.28.4 Objective

The objective of this policy is to record events and generate evidence.

## 2.38.5 Roles and Responsibilities

* All users are required to understand this policy and put into action.
* Head, Information Security and Head, IT is responsible for implementing this policy.
* Head, Information Security is expected to ensure adherence to this policy
* Internal Audit – IS Audit is responsible for auditing the implementation of this policy.

## 2.38.6 Policy Details

* The XXXX shall audit, log, and monitor access and events to detect, report, and guard against:
* Network vulnerabilities and intrusions
* Performance problems and flaws in applications
* Security violations
* Data loss
* Unauthorized access to confidential data, privileged information, etc.
* Breaches in confidentiality and security of confidential data
* Degradation or loss of information integrity (e.g., improper alteration or destruction of confidential data) etc.
* Audit logs shall be enabled on systems in-order to record user activities, exceptions and information security events and preserve them as set out in the retention schedule to assist in future investigations. Audit logs shall include:
* Type of event
* Dates, time, and details for key events, example: log-on and log-off
* Records of successful and rejected system, data or other resource access attempts
* Identity or name of affected data, system component, or resource
* Information about the event (for example, files handled) or failure (example, error occurred and corrective action taken).
* The account details of the administrator or operator who is involved.
* The processes that are involved.
* The audit trail history is retained for at least 12 months, with a minimum of 6 months immediately available for analysis through the log management tool. Only Authorized personnel can retrieve customized reports on demand from the logging and reporting interface of the log monitoring tool used by the XXXX.
* Different log monitoring tools are used to perform monitoring activities according to security requirements provided by Information Security team. At minimum, the log monitoring tool shall have the following functionalities:
* Ability to collect and co-relate logs from different types of systems and databases.
* Monitor server logs, Memory and Disk Utilization, Services, Windows Services, Processes, Custom scripts, URLs (HTTP⁄ HTTPs), Files⁄ Folders across multiple Operating systems.
* Supports Windows, Linux, Solaris, HP UX, IBM AIX servers and other operating systems and hardware.
* Monitors server virtualization logs and supports VMware and Hyper-V.
* Monitors essential Microsoft services for applications like, Exchange, Active Directory, and MS SQL.
* Monitors network devices logs like routers, switches, firewalls, and other devices to analyze traffic usage.
* Stores the log information in a raw format.
* Access to audit logging systems, audit records and system audit tools shall be limited to those with a job-related need according to the Access Control Policy to protect against possible misuse of the tools or compromise to the audit records.
* System Administrators are prohibited from erasing or de-activating logs of their own activities.
* System Administrators are prohibited from disabling logging activity. Disabling audit logs or tampering with audit log information is treated as a serious offence in the disciplinary policy and may result in immediate dismissal.
* System clocks shall be synchronized always. Any changes to time settings on the XXXX’s systems shall be in accordance with the change management process. Information Technology shall synchronize all system clocks with a real-time clock (NTP Server) set to Coordinated Universal Time (UTC) to support tracing of activity timelines.
* The Information Security team is responsible for reviewing the results of monitoring activities on a weekly basis for all identified system components and alerts received on a daily basis. If a reviewer sees an alert or finds an unauthorized activity, it is treated as an exception and followed up by:
* Completing a security incident report
* Opening a service ticket
* Consulting with the Information Security Forum

# ENFORCEMENT

Implementation of these policies will be verified from time to time by Information Security, Internal Control and Internal Audit. Any user or employee found to have violated this policy shall be subject to disciplinary action including termination of employment.

# CONTROLS

Objectives shall be agreed on an annual basis, supported by a set of key performance indicators (KPIs), with milestones and targets. These measures shall be reported to the Information Security Steering Committee for review.

# KEY PERFORMANCE MEASURES

This Information Security Policy shall be reviewed annually by the Chief Information Security Officer and agreed by the Information Security Steering Committee to ensure it remains fit for purpose.

# REFERENCES

* BS ISO/IEC 27001:2013 Information technology — Information Security Management System — Requirements
* BS ISO/IEC 27002:2013 Information technology — Code of practice for information security management
* PCI DSS version 3.2.1
* CBN risk-based cybersecurity framework and guidelines for DMBs & PSPs
* XXXX - IT Policies and Procedures
* XXXX - Information System Control Policy
* RUSecure – Information Security Policies Evaluation

# REVISION HISTORY

|  |  |  |
| --- | --- | --- |
| **Date of Change** | **Name** | **Summary of Change** |
|  |  |  |

**Appendix A – Third Party Access Form**

|  |  |
| --- | --- |
| Access to the XXXX’s XXXX information systems and network has been requested by : |  |
| Signature & Date |  |

**ACCESS DETAILS**

|  |  |
| --- | --- |
| **Access is granted to:**  [specify Name and Contact details of Company/Individual, including location] |  |
| **Access is granted in the form of:**  [specify access details e.g. Username/ Password] |  |
| Number of users: |  |
| Access is granted to the following data/ systems/device(s): |  |
| Remote access method granted will be:  [specify access details (e.g. VPN/dial-up))] |  |
| Domain/applications available via this system |  |
| Protection methods in use to protect connection/time |  |
| Protection methods in use to protect domain/other application use |  |
| Protection methods in use to protect organisational sensitive data |  |

**SECURITY CONDITIONS**

* Access to XXXX’s systems and data is granted for approved purposes only. The use of this access for personal use or gain is strictly prohibited.
* Access to the XXXX’s information & network facilities will not be provided until a signed copy of this contract has been returned to the Network Security Team.
* The Third Party is permitted only to use access methods meeting appropriate protocols.
* The Third Party will inform the XXXX in writing of appropriate staff changes in relation to access to XXXX systems.
* The XXXX reserves the right to monitor activity, revoke access and audit contractual responsibilities.
* Where the Third Party has direct or indirect access to data or information owned by the XXXX, this information must not be copied, divulged or distributed to any other party.
* On the completion of this contract the third Party must return all data belonging to XXXX.
* Any suspected security breaches or other incidents must be reported in a timely manner to the vendor’s contact person.
* The Third Party will at all times be held responsible for any activities that occur on the XXXX’s network and applications using any unique user IDs granted.
* The Third Party is solely responsible for ensuring that any username(s) and password(s) that they are granted remain confidential and is not used by unauthorised individuals.
* The Third Party agrees that once access has been gained to the network, system or data, activities will be restricted to that system or data and to resolution of the issue(s) or provision of the agreed service that gave rise to the requirement for access on that occasion. These will be detailed in this agreement, or in an attached contract or Service Level Agreement.
* The Third Party shall not use, divulge or communicate any personal information including information relating to the Client's finances, business or commercial affairs, or information of a technical nature, made accessible to the supplier as a consequence of this agreement, which it shall treat as confidential and safeguarded accordingly.
* The Third Party shall ensure that its employees, agents, subcontractors and any third parties to whom data or information is disclosed or made accessible under this agreement are aware of the requirement to maintain the security and confidentiality of any such data and information
* Workstations/laptops that are used to display the XXXX’s data should be located in such a way that confidential information is not displayed to unauthorised persons or the general public.
* The XXXX reserves the right to increase security thresholds if future security risks are identified.
* The Third Party is expected to notify the System Owner once a remote access session has been completed.
* All Third party hosts connected to the XXXX’s network must:
* Use the most up-to-date anti-virus/anti-spyware/anti-malware software available
* Be protected by a Corporate or private Firewall
* Be up to date with operating system patches
* Not be made available for use to unauthorised third parties
* Be available for inspection by IT Services or the Information Security Manager if requested.

(3RD PARTY COMPANY’S NAME AND ADDRESS)

**Signed for on behalf of 3rd PARTY**

**NAME: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Of: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Signed for on behalf of XXXX**

**NAME: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Of: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Head, IT: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Head, Information Security: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**