EQUITY BANK UGANDA LIMITED

INFORMATION SECURITY POLICY

1. Introduction

As a modern, forward-looking business, Equity Bank Uganda Limited ("Equity" or "EBUL") recognises at senior levels the need to ensure that its business operates smoothly and without interruption for the benefit of its customers, shareholders and other stakeholders. In order to provide such a level of continuous operation, Equity is implementing an Information Security Management System (ISMS) in line with the International Standard for Information Security, ISO/IEC 27001.

This information security policy forms a key part of our set of controls to ensure that our information is protected effectively and that we can meet our obligations to our customers, shareholders, employees and suppliers.

1.1. Policy Objectives

- To ensure business continuity, minimize business risk and maximize return on investments and business opportunities.
- To protect Equity's ability to function and enable a safe operation of applications implemented on IT systems.
- To protect data collected and used by Equity while also safeguarding the technology used.
- To ensure the preservation of confidentiality, integrity, and availability of systems and information used by Equity. These three principles compose the CIA triad:

    - **Confidentiality** involves the protection of assets from unauthorized entities.
    - **Integrity** ensures the modification of assets is handled in a specified and authorized manner.
    - **Availability** maintains a state of the system in which authorized users have continuous access to said assets.

1.2. Applicability of Policy

- This policy applies to all information, information systems, networks, applications, locations within Equity.
- This policy applies to all persons employed by or under contract with Equity.

1.3. Audience

- This policy applies to all persons employed by or under contract with Equity.
- All staff relevant to the information security management processes shall remain informed on the contents and all updates that to this policy.

2. Scope

This policy shall provide guidelines on the following metrics pertaining to the information security management within Equity Bank Uganda Limited.

- **Top Management commitment to Information Security**
- **Information Security Requirements**
- **Information Security Management System (ISMS) Plan & Objectives**
- **Risk Assessment**
- **Information Security Guidelines and Standards**
    - Identity and Access Management
    - Clear Desk and Clear Screen
    - Malware Management
    - Logging and Monitoring
    - Vulnerability and Patch Management
    - Information Security Incident Response
    - VPN Acceptable Use
    - Threat Management
    - Password Management
    - Data Access
    - Key Management and Card Data Encryption
    - Remote Access
    - Physical Security
    - Card Data Protection
    - Network and Infrastructure Configuration
    - Acceptable Use Cloud computing
    - Information Classification and Handling
    - ICT Change management
- **Awareness Plan and Program**
- **Non-compliance**

Appendix:

Security Awareness Tips

Protect yourself from fraud.

Digital technology has made our lives easier and more convenient, but it's also made it easier for fraudsters to trick and cheat us. Learn how to spot and stop fraud, and what you can do to prevent fraud on your accounts.

Tips to stay fraud safe

Secure your personal and financial information.

Fraudsters can attempt to take over your account if they can impersonate you and gain access to your personally identifiable information. Social engineering, hacking, malware, email compromise are some deceptive ways through which they can obtain this information.

Phishing / Voice Phishing

- If you receive a suspicious email or phone call claiming to be from the us, forward the email with the attachments included or report the incident to infoug@equitybank.co.ug
- You should then delete the email immediately Please call our Customer Service Hotline immediately if you suspect any unauthorised access or transactions on your account.

Spot the warning signs

- When making online purchases, always double-check the website's authenticity.
- Look at the address bar: it is considered secure if the URL begins with "https" instead of "http", and has a small closed lock symbol.
- Red flags include spelling or grammatical errors; time-limited offers, flash sales or discounted pricing; unusual payment requests like bank transfer; products that have no reviews, bad reviews, or only positive reviews written in a similar way.
- If you're shopping on an online marketplace, check the website's safe buying guide before making a purchase. Some online marketplaces will not offer any protection if you make payment outside of the platform.

Stop suspicious activity

- Be vigilant at all times. Never open unexpected emails asking you to click on a link to arrange a delivery or make payment.
- Always make the effort to double-check the facts and verify that the other party is legitimate before making any payments. Search for the retailer online with terms like "scam" or "complaint" and look for reviews by other consumers.
- Do not authorise payments unless you are sure that the other party is legitimate.

Report the incident

If you suspect any suspicious activity, report the incident to local authorities or your bank immediately.