Revision History (Version 4.0)

Ref	Date	Change
Version 1	June 2009	Updated security policy framework
Version 2	Dec 2013	**Update:** Personal computers controls Section 2
Version 3	October 2016	**Update:** – Change management controls – Section 4.5.4 – Incident management – Section 4.5.5 – Remote access controls Section 5.5 – Removal of the word 'diskette' reference within this document
Version 4	June 2021	**Update:** – Vision statement Section A.1 - amended to make reference to The Kenya Data Protection Act (2019), CBK Guidance Note on Cybersecurity (2017 – Third party security Section B amended to make reference to The Kenya Data Protection Act 2019 – Minimum password length (under User password responsibilities) amended to 8 characters. Section I.2 – Added requirements for secure telecommuting. Section I.6.1 - Added ISO 27001 clauses Section A.10 -Clause 6.1.1 Section E.2 -Clause 11.2.3 Section G.7-Clause 12.4.4 Section J.1 – Clause 14.2.7 Section J.4 -Clause 14.2.8 Section K.1 -Clause 16.1.3 – Amended section A.5 (Exceptions) to capture approval matrix for policy exceptions. – Amended section A.10 (Responsibility for security) to capture responsibilities for Board, Senior Management, IT Security office, Risk and Compliance, Internal Audit.

1. Vision statement

It is the policy of Housing Finance Group (herein referred to as "HFCB") to establish and maintain comprehensive protection and clear accountability for all its information assets and resources. This includes information assets that are proprietary to HFCB, private to HFCB's customers and all other private and proprietary information assets and resources that, if subject to inadvertent or unauthorized disclosure, would likely cause financial, legal, regulatory, or reputation damage to HFCB. Comprehensive protection for all HFCB information assets and resources will be accomplished through a system of controls that is commensurate against the inherent risk to and/or value of the information.

The Information Security policies contained within this document were created in response to business needs, changes in the regulatory environment, Payment Card Industry Data Security Standard (PCI-DSS), CBK National Payments Systems and third-party requirements (e.g., credit card processors), Kenya Data Protection Act (2019), CBK Guidance Note on Cybersecurity (2017). Interpretation as to the spirit and intent of this policy is the responsibility of HFCB's Management.

2. Scope and applicability

This policy applies to all computer and network systems owned by and/or administered by HFCB, or operated by a third party for the benefit of HFCB. This includes all locations where HFCB's business is conducted, including Data Centers, Corporate Offices and Customer Contact Centers. Similarly, this policy applies to all operations managed by HFCB, and all computers, networks, devices used to connect to HFCB, operating systems (regardless of size), data systems (e.g., Lightweight Directory Access Protocol [LDAP], Data Base Management Systems [DBMS], etc.), and all application systems whether developed in-house or purchased from third parties. This policy also covers all private and proprietary information assets and resources included in documents, conversations and all electronically stored, processed, transmitted, printed, and faxed information. Lastly, this policy applies to all regular and temporary, part-time or full-time employees, as well as contract personnel, consultants, suppliers, vendors and other non-HFCB employees.

3. Purpose

To ensure that our ICT systems, infrastructure and environment continues to operate, and that confidentially, integrity and accuracy of information is maintained, a high-level information security policy is required. For this reason, this policy has been introduced and everyone is expected to read it and to ensure that its provisions are complied with. The purpose of the Policy is to *protect the company's information assets"* from all threats, whether internal, external, deliberate or accidental ensuring that:

1. Information is protected against unauthorized access.
2. Highest level of confidentially and integrity of information is maintained.
3. Establishing effective procedures, that ensures good corporate governance and internal controls environment.
4. Regulatory and legislative requirements are met.
5. High-level business continuity plans are formulated, tested and maintained.
6. Information security training is availed to all Staff.
7. Considerations are placed on the legal liability of the company in order to avoid poor awareness of the regulations that can cost the company dearly.
8. All Information security breaches, actual and suspected are immediately reported, and investigated by the IT Security office.
9. Business requirements for the availability of information and information systems will be met.

Standards and procedures will be produced to support the policy. These may include virus control, passwords and encryption standards, data maintenance standards, change control procedures etc. and they will be enhanced from time to time it to conform to industry best practices.

The role and responsibility for managing information security will be performed by Risk & Compliance Division which will include formulating, enhancing, and maintaining the policy, providing advice and guidance on its implementation. Internal Audit will however ensure adherence and monitoring of the policy, ensuring it is within the industry best practices. Divisional Directors and Managers will directly be responsible for its implementation within their business areas, and ensure total compliance by their Staff. It is the responsibility of each employee to adhere to the policy.

4. Accountability

The successful implementation of HFCB's Information Security policy cannot be achieved without company support; therefore, all HFCB employees are accountable for compliance with this policy. Management is accountable for implementing and supporting this policy. All employees who in anyway deploy, support, maintain, or contract services in technology are accountable for adhering to this policy and reporting suspected policy breaches/issues/problems to his/her management. All HFCB private and proprietary information is provided to HFCB employees, contractors, vendors and other authorized persons in strict confidence. Those with access to HFCB private and proprietary information are accountable for safeguarding such information as described within this policy, and detailed further in associated implementation standards and guidelines, and procedures.

5. Accountability

It is recognized that with certain technologies, systems, platforms, products, etc., strict compliance with the HFCB's Information Security policy may not be practical or reasonable to meet HFCB's business needs.

Exceptions may be made where the cost of compliance exceeds the overall risk or business benefit. If an exception is needed, the exception process must be followed to document the noncompliant item and plan for risk mitigation. Exceptions include a decision to eliminate, mitigate, tolerate, or escalate the risk. Once the inability to comply with the security policy has been established, a strategy must be documented to address the issue(s), including (at a minimum):

- An explanation of the risk(s);
- Rationale as to why the risk(s) should be tolerated or mitigated rather than eliminated;
- Alternate controls necessary to do so; and
- Endorsement/Approval by the management

Ultimately, any choice other than elimination must be raised in advance by the Chief Information Security Officer, supported by Head of Risk and Compliance, Head of Internal Audit and approved by the Chief Operations Officer and Group Chief Executive Officer.

6. Accountability

In the absence of an approved exception, failure to comply may be considered a violation of HFCB's policy and may result in appropriate disciplinary action leading up to termination of employment or contract.

7. Accountability

Policy

The Information Security policy is a set of generalized statements describing the overarching information protection objectives of HFCB. The statements reflect HFCB's accepted practices for performing internal control, for addressing current and future information protection goals, and are written in a manner so they do not require frequent revision.

Implementation Standards & **Guidelines**

For each security policy statement, a set of implementation standards and guidelines may exist which further detail leading practices that must be followed to adhere to the policy.

Procedures

Procedures elaborate the intentions expressed in policy statements and implementation standards and guidelines by providing actionable steps that facilitates achieving information protection goals. As a written course of action, procedures may take the form of installation manuals, user guides, checklists, standard operating procedures, and other process documents.

Implementation standards and guidelines and procedures as well as Acceptable Use Policies for HFCB

Information and Information Resources (e.g., laptop, mobile devices) are documented separately. The Information Security policies are separate from, but work in conjunction with, the Data Classification and Handling Policy in protecting information assets.

8. Accountability

All HFCB employees and relevant third parties with access to HFCB's information assets must acknowledge in writing that they have read and understood the HFCB Information Security policy.

9. Accountability

This policy is intended to review issues of safekeeping and confidentiality of information resources, identify risks, raise consciousness with the Staff and, where appropriate, develop policy statements, advisories, guidelines and procedures.

The HFCB Risk Management Committee (RMC) with representation from all divisions of the company and is charged with execution and managing the information security process. The intention is to build consensus among all Staff members, promote common definitions, and compile good practices and checklists in the form of this policy document.

10. Responsibility for Security

The successful operation of this policy cannot be achieved without the wholehearted cooperation of every employee and support of Senior Management and the Board. It is therefore imperative that all stakeholders including employees, third parties, senior management, etc. are aware of it and other instructions derived from it and as such:

- The Board of Directors - All HFCB Board members should understand the nature of the Bank's business and the Information security related risks involved. The Board will approve the Information Security policy and associated strategies and roadmaps. The Board will also ensure adequate budgetary allocation for the full implementation/ execution of the policy.
- Senior Management – Senior Management of the Bank is responsible for implementing the Bank's business strategy, risk appetite and manage threats. As such, the Senior Management through the HFCB Risk Management

Committee (RMC) are required to implement the Board approved Information Security policy and associated strategies and roadmaps.

- IT Security office/Chief Information Security Officer (CISO) – The IT Security office is responsible for creating/ promoting an organizational culture of shared information security risk awareness and ownership. This role will oversee and implement the Bank's Information Security management program and enforce the approved Information Security policy. The IT Security office will be responsible for providing advice to the HFCB Risk Management Committee (RMC) and Line Management as necessary on all aspects of IT Security. This will include helping line managers to develop standards and procedures, as necessary, to explain and amplify the Information security policy in their respective areas.
- Risk and Compliance will be the custodians of the Information Security policy. They will also conduct periodic reviews across the organization to ensure that all provisions of the information security policy are properly enforced and complied with.
- Internal Audit Division will be responsible for reviewing and providing assurance on the adequacy of this policy and recommend improvements where deficiencies are found. They shall also provide assurance on compliance with the policy requirement on people, processes and systems.
- All employees and third parties shall comply with the policy including related standards and procedures. Employees who fail to comply with these directives will be liable to disciplinary action.
- Non-disclosure of organization's confidential information as well as compliance with legal and regulatory requirements on protection of personal will be applicable even after employee's exit from the organization or termination of contract with third parties. Employees and third parties will be required to commit to this responsibility during the onboarding process or at system access provisioning stage.
- Contracts with external organizations will include a clause stating the requirement that they need to follow the Information Security Policy and other appropriate directives. Any failure to do so will be regarded as a breach of contract.
- Any deficiencies or room for improvement in this policy should be pointed out to the HFCB Risk Management Committee (RMC). The co-operation of all employees is highly required to make the policy as effective as possible.

Approvals		
Approved By	**HFCB Board**	**July 2021**

Effective Date			**Next Review Date**	
Date	**Month**	**Year**	**Month**	**Year**
30th	**July**	**2021**	**July**	**2023**