BRAC UGANDA BANK LIMITED INFORMATION SECURITY POLICY

1.0 Introduction

Information is one of the most valuable assets of the bank, and its protection is essential to maintaining the trust of our customers, meeting regulatory obligations, and supporting our operational integrity and reputation. As threats to information security continue to evolve in complexity and frequency, it is critical that all bank staff, contractors, and third parties understand their roles in safeguarding the bank's information assets.

This Information Security Policy establishes the framework for maintaining the confidentiality, integrity, and availability of information across the bank. It defines the bank's commitment to managing information security risks, complying with legal and regulatory requirements in alignment with ISO/IEC 27001:2022 standards.

The policy applies to all staff, systems, processes, data, and third-party services that interact with the bank's information assets, whether digital or physical. All users are required to comply with the principles and controls outlined in this policy to ensure the security and resilience of the bank's information environment.

1.1 Objectives

This policy manual provides all bank staff with the primary objectives of the Information Security Policy including the below:

- Safeguard the bank's information assets by ensuring their confidentiality, integrity, and availability, while implementing a risk-based approach to manage information security threats.
- Promote compliance with applicable laws, regulations, and contractual obligations—especially in data protection, privacy, and financial services—while fostering a security-aware culture among employees, contractors, and third parties.
- Enhance business continuity by minimizing the impact of security incidents through effective incident response and disaster recovery strategies.