INFORMATION SECURITY POLICY

Version 1

CBG
CONSOLIDATED BANK GHANA

CONFIDENTIALITY CLAUSE AND DISCLAIMER

CONTENTS

1.INTRODUCTION

CBG's Information Security Management System (ISMS) has been developed based on the leading industry standard for information security management and Cyber Security – ISO/IEC 27001 and ISO/IEC 27032.

The ISMS policies and procedures will govern the development, implementation and continual improvement of the ISMS.

CBG's Executive Management commitment to the ISMS will be demonstrated by taking responsibility for the ISMS and allocating appropriate resources to ensure adequate maintenance of information security at CBG**.**

The objectives of CBG's ISMS are as follows:

a. To gain the trust of CBG's customers, partners, and other relevant stakeholders
b. To add value to the organization and demonstrate that CBG is committed to creating and sustaining a culture of security awareness that ensures the protection of its client's and partner's information assets
c. To globalize its operations and distinguish itself from competitors
d. To ensure continuity of business in adverse or disruptive situations
e. To ensure that the confidentiality, integrity, and availability of all information assets of CBG are not compromised
f. To ensure that all information assets of CBG continue to operate securely and follow the ISO/IEC 27001 and ISO/IEC 27032 security requirements
g. To ensure that information is secure from unauthorized access
h. To ensure that CBG complies with all the applicable legal and regulatory requirements. (For example, the Bank of Ghana Cyber and Information Security Directive for Financial Institutions, Data Protection Act, 2012, etc.)

1.1. Scope

The scope of this policy encompasses all assets of CBG information/information assets, employees, contractors and third-party personnel.

This policy is applicable to the following:

a. All information including but not limited to customer information, CBG employees and related information generated, processed and stored by the various entities to perform their activities and deliver their services.

b. All information assets that process the aforementioned information at the Bank. Information assets may include, but are not limited to; hardware assets, software assets, services assets, people assets and paper assets.

c. All employees, contractors and third-party personnel of CBG accessing the Bank's information processing facilities. CBG's information processing facilities include, but not limited to; Data Centres, offices, work areas, secure areas, Critical Infrastructure Rooms (CIR) and telecommunications facilities.

2.ORGANIZATION OF INFORMATION SECURITY

2.1. Management direction for information security

2.1.1. Commitment to satisfying applicable requirements

Commitment to information security extends to senior levels of CBG and will be demonstrated through this Information Security Policy and the provision of appropriate resources to establish and develop the ISMS.

Management of CBG shall be committed to satisfying all applicable legal, regulatory and contractual information security requirements and those stated under this policy.

2.1.2. Commitment to continual improvement

CBG's policy with regard to Continual Improvement of the ISMS is to:

- Continually improve the effectiveness of the ISMS across all areas within the scope
- Enhance current processes to bring them into line with good practice as defined within ISO/IEC 27001
- Achieve ISO 27001 certification and maintain it on an on-going basis
- Increase the level of proactivity (and the business perception of proactivity) with regard to the on-going management of information security
- Achieve an enhanced understanding of, and relationship with, the business units to which the ISMS applies
- Review relevant metrics on an annual basis to assess whether it is appropriate to change them, based on collected historical data and feedback from relevant sources
- Obtain ideas for improvement via regular review meetings with stakeholders
- Review ideas for continual improvement at regular management meetings in order to prioritize them and assess timescales and benefits

2.1.3. Information Security in Project Management

a. All projects undertaken within CBG that consume information and IT assets or involve areas of information risk, must address privacy, information risk and security concerns and should include an Information Security risk and Data Privacy Impact assessment at an early stage of the project to identify necessary controls.

3.MOBILE DEVICE POLICY

a. Only approved mobile devices may be used to access CBG Information and IT Assets.

b. All mobile devices must, at a minimum, be password protected in accordance with the Password Security Policy Manual.

c. The devices must remain current with anti-malware definitions, must be kept current with the operating system and third-party software security patches, and must run a personal firewall.

d. When connecting to CBG networks from remote locations, only do so through the CBG approved Virtual Private Network (VPN).

e. All CBG data stored on these devices must be encrypted using CBG approved encryption standard.

f. Third party personnel shall not connect their computing devices to the CBG's network unless the device and configuration requirements of CBG are met and approved by the CISO.

4.TELEWORKING

a. Users must only use CBG configured computers to access or connect to the CBG network. Home PCs, personal laptops or other non-CBG computers are prohibited. Only users that have a justifiable business case for remote access will be authorized for access by the information owner.

b. Security of all laptop computers must include:

   i. Encryption of storage media (when possible).

   ii. Log-on passwords.

   iii. Protection of data being transmitted to/from the mobile device e.g. Virtual Private Network (VPN), Secure Socket Layer (SSL) or Pretty Good Privacy (PGP); iv. Mobile or remote users must be trained specifically in security measures to be taken for remote access.

5.HUMAN RESOURCE SECURITY

Information security responsibilities shall be addressed prior to employment in adequate job descriptions and in terms and conditions of employment. All candidates for employment, contractors and third-party personnel shall be adequately screened, especially for jobs defined as sensitive. Employees, contractors and third-party users of information processing facilities shall sign an agreement on their information security roles and responsibilities.

5.1.1. Information Security Awareness, Education and Training

a. All employees, relevant contractors and third-party personnel shall receive information security training.

b. All employees, relevant contractors and third-party personnel shall undergo an annual information security refresher training and an acknowledgement of the completion of same shall be maintained.

6.ASSET MANAGEMENT

6.1.1. Acceptable Use of Assets

a. All employees, contractors and third-party personnel shall be responsible for handling the information or information assets per the classification of the asset.

b. All employees, contractors and third-party personnel shall be responsible for safeguarding the Bank's sensitive information from disclosure to unauthorised parties.

7.ACCESS CONTROL

Access to information/information assets, information processing facilities, systems, applications equipment and network devices shall be restricted per the valid business requirements, user's job responsibility and information security requirements. Formal procedures shall be in place to control the allocation of access rights.

Except for the publicly held information/publicly available information assets, access to all other information/information assets, systems, applications, equipment and network devices shall be granted based on a Need-to-Know and Need-to-Have basis and after the requisite approval is obtained.

7.1.1. Access to Networks and Network Services

a. End users (including but not limited to employees, contractors and third-party personnel of the Banks' information systems, applications, equipment and network devices) shall not deliberately conceal or misrepresent their network identity through use of anonymous proxy or by other means.

b. The Bank's networks shall be segregated from the networks owned by other organizations and public networks.

7.1.2. Management of Passwords of Users

a. All information/information assets, information systems, applications, equipment and network devices shall be configured with parameters for password management, as specified in the Password Management Standards.

7.1.3. Use of Passwords

a. Passwords shall never be shared or revealed to anyone other than the authorized user.

b. Users shall not store fixed passwords in any computer files, such as logon scripts or computer programs, unless the passwords have been encrypted with authorized encryption software.

c. Passwords shall not be written down however, critical system passwords that need to be written down should be subject to a transformation process that conceals them, or they are physically secured, such as placed in a locked file cabinet.

d. Users shall keep their User IDs and corresponding passwords confidential and refrain from sharing them with others.

e. The Bank's information systems, applications, equipment and network devices shall be configured to ensure that displaying passwords are masked, suppressed or otherwise obscured such that unauthorized parties may not be able to observe and/or subsequently recover them.

f. All passwords must meet complexity requirements set forth by the password guidelines.

8. CRYPTOGRAPHY

a. Encryption shall be adopted for information assets based on the criticality of the information. Unless required by regulatory requirements, standard encryption technology shall be deployed for encryption

b. The Banks shall ensure protection of sensitive data through:

i. Encryption of sensitive data stored on laptops and desktops through full or partial disk encryption. This shall also address data storage on removal devices such as USB drives and hard disks. ii. Encryption of emails containing sensitive information and being sent to the external environment.

iii. Encryption of sensitive data stored on all backup devices such as tapes, hard disks.

iv. Encryption of sensitive data during transit.

9. PHYSICAL AND ENVIRONMENTAL SECURITY

Information assets shall be physically protected from unauthorized access, misuse, damage and theft. All of the Bank's information processing facilities shall be adequately protected from physical and environmental threats.

10. CONTROLS AGAINST MALWARE

a. Detection, prevention and recovery controls shall be implemented in all information systems, applications, equipment, network devices and mobile devices to protect against malicious code.

b. All devices must remain current with anti-malware definitions

c. All files received from any source shall be scanned for viruses before execution or usage.

d. Backup storage media should be scanned for viruses before any files are restored to the production system/environment.

11. INFORMATION BACKUP

a. Information backup and restoration procedures shall be established and implemented to ensure the availability of business information.

b. Backup media shall be encrypted, depending on the classification of the data stored on it.

12. MANAGEMENT OF TECHNICAL VULNERABILITIES

a. All security vulnerabilities of information systems, application software, system software and products shall be identified and documented and the exposure to such vulnerabilities shall be evaluated.

b. All Vulnerability Assessments (VA) shall be conducted on a periodic basis by the Information Security Department or authorized Third Parties.

c. Penetration Testing (PT) shall be performed for all external facing and critical systems, equipment and network devices, utilized for providing services, on an annual basis.

13. EXCHANGE OF INFORMATION

13.1.1. Information Transfer Policies and Procedures

a. All employees, contractors and third-party personnel shall take all possible care to avoid information disclosure while discussing the Bank's information in public places such as in building lobbies or on public transportation.

b. All employees, contractors and third-party personnel shall exchange the information classified as 'Highly Confidential', 'Confidential' and/or 'Internal' for specified duration, based on the business requirements with authorized personnel only. The relevant information, thereafter, shall be deleted after the confirmation from the specific individuals.

c. Documents and removable media carrying information of Highly Confidential or Confidential classification shall be couriered through an authorized personnel.

d. The authorized personnel involved in the transport is required to sign a Non-disclosure Agreement

14. ELECTRONIC MESSAGING

a. Electronic messaging solution deployed in the Bank shall have protection from unauthorized access and modification.

b. Employees shall not employ any electronic mail addresses other than official electronic mail addresses for the Bank's business matters.

c. Unless the information owner or originator agrees in advance, or unless the information is clearly public in nature, employees shall not forward electronic mail to any address outside the Bank's networks.

d. All electronic mail messages shall be retained for future reference.

e. Employees shall not send or forward any messages through the Bank's information systems that may be considered defamatory, harassing, or explicitly sexual, or would likely offend someone on the basis of race, gender, national origin, sexual orientation, religion, political beliefs, or disability or that may contribute to a hostile work environment.

f. Employees shall not send or forward any messages through the Bank's information systems that contain copyrighted content that is not the intellectual property of the Bank.

14.1.1. Confidentiality or Non-disclosure Agreements

a. All users, including but not limited to CBG employees, contractors and third-party personnel shall sign confidentiality or non-disclosure agreements. HR function shall be responsible for ensuring that all users sign confidentiality agreements.

b. Without specific written exceptions, all programs and documentation generated by, or provided by any employee for the benefit of CBG, are the Bank's property and all the employees providing such programs or documentation shall sign a standard Non-

Disclosure Agreement (NDA) or a confidentiality clause authorized by the Bank's Legal Department.

c. Whenever communication/interaction with third parties necessitates the controlled release of the Bank's sensitive information; a standard Non-Disclosure Agreement (NDA) or a confidentiality clause authorized by the Bank's Legal department shall be signed with the third party prior to the release of the information. Third parties shall comply with the Third-Party Information Security Policy.

15. INFORMATION SECURITY INCIDENT MANAGEMENT

All employees, contractors and third-party users shall be made aware of the event and escalation procedures for reporting the different types of events and weakness that might have an impact on the security of the Bank's assets. Employees, contractors and third-party personnel shall be required to report any information security events and weaknesses as quickly as possible to the Information Security Department .

a. All incidents shall be categorized based on their criticality per the established guidelines.
b. The notification and resolution timelines shall be defined based on the incident category.
c. The Bank shall establish an escalation process for the timely resolution of incidents.
d. An action plan shall be developed and root cause analysis performed for all incidents reported to prevent recurrence.
e. Appropriate forensic methods shall be applied, whenever required, to collect evidence in the course of investigation of information security incidents. This shall be coordinated by Internal Control Department and done by a trained and authorized forensics investigator where necessary.