PremiumTrust Bank

Information Security Policy Manual

PTB/ICS/22/0001
Version 1.0

Classification: Internal

Document Number: PTB/ICS/22/0001
Policy Status: Approved

Date Approved: March 2023

Document Control Sheet

Version and Update History

Date	Document Version	Document Revision History	Document Author/Reviser
September 2022	1.0	Document creation	Information & Cyber Security

Change Control

Change Clause/Frequency
The contents of this document are subject to change control on a twelve (12) months review cycle.

Table of Contents

1. Information Security Policy and Security Organization

1.1. Introduction

Information and supporting processes, systems, and networks are important business assets. Confidentiality, integrity, and availability of information are essential to maintain a better competitive edge, cash flow, profitability, legal compliance, and reputation. Information Security is the preservation of the following 3 characteristics of information:

- Confidentiality – ensuring that information is accessible only to those authorized to have access.
- Integrity – safeguarding the accuracy and completeness of the information and its associated processing methods. This refers to protection against unauthorized modification.
- Availability – ensuring that authorized users have access to information and associated information processing systems when required.

This policy specifies the requirements needed to ensure the confidentiality, integrity, and availability of PremiumTrust Bank's information resources.

Additionally, when information is transmitted or communicated, the following security principles also need to be complied with:

- Authentication/Identification – ensuring that the identity of the user/entity can be positively verified.
- Non-repudiation – ensuring that the sender and/or recipient cannot deny sending or receiving the information concerned.

1.1.1. The Importance of Information Resources to PremiumTrust Bank

Information resources are vital assets of PremiumTrust Bank as the Bank's other business assets. Information resources are the lifeblood of the Bank and shall therefore be

adequately protected against all risks. The protection of PremiumTrust's information resources is critical to PremiumTrust's continuity.

Need for Policy

PremiumTrust Bank's information resources are critical to delivering quality services to customers and complying with regulatory requirements. PremiumTrust Bank shall therefore ensure that such information resources are adequately protected when used by all authorized parties. To protect PremiumTrust Bank's information resources during internal and external use, in addition to conforming to statutory and contractual requirements regarding its information, Information Security is one of PremiumTrust Bank's prime responsibilities to protect and secure these vital assets. This responsibility is shared by all employees of PremiumTrust Bank.

1.1.2. Management's Commitment to Information Security

PremiumTrust Bank is committed to mitigating risk and meeting the compliance requirements of its services. To this end, the Information Security Policy Manual has been documented and approved to clarify business interpretations and implementation requirements of the Bank's Information Security. Information in all its forms, including information about employees, customers, and products, is amongst the most valuable assets of the Bank. The security (confidentiality, integrity, and availability) of that information is key to PremiumTrust Bank's successful discharging of its responsibilities to customers and stakeholders. Therefore, the security of PremiumTrust Bank's information, and the systems, and programs that facilitate its use is a responsibility shared by every employee of the Bank. Every employee of PremiumTrust Bank has an obligation to ensure the confidentiality, integrity, and availability of PremiumTrust Bank's information resources.

Management is primarily responsible for implementing controls throughout the organisation, in line with corporate governance tenets. Management realises the strategic

importance of Information Security within the operations of the Bank. Management hereby gives full support and commitment to the enforcement of all aspects of Information Security on a corporate level as well as that of every individual member's level. This commitment is formulated in terms of the policy statements in the information security policy manual.

1.2. Overview of the PremiumTrust Bank Information Security Policy

1.2.1. Purpose

PremiumTrust Bank has established this Information Security Policy to provide high-level guidance and to set the minimum requirements that must be followed to maintain the required level of Information Security within the Bank.

The purpose of the Bank's Information Security Policy is to specify the measures required to protect PremiumTrust Bank's information resources from all types of threats, whether internal or external, deliberate, or accidental.

This document focuses on PremiumTrust Bank's corporate policy for Information Security. Specific policies, standards, procedures, and guidelines to facilitate the implementation of this high-level framework shall be established within groups and business units.

1.2.2. Compliance Requirements

The Information Security Policy applies to PremiumTrust Bank and all its employees, including temporary staff, contractors, service providers, and consultants utilizing PremiumTrust's information resources. The policy covers the data networks, servers, and personal computers (stand-alone or network-enabled) located at PremiumTrust's head office and branches. This includes systems that are under the jurisdiction and/or ownership of PremiumTrust Bank, and all personal computers and or servers authorized to access PremiumTrust Bank's data networks.

1.2.3. Maintenance and Review

Information on currently valid policies, standards, and specifications can be obtained from the Information & Cyber Security department. All standards and specifications are subject to revision, and all parties are encouraged to investigate the possibility of applying the most recent edition of the policies defined in this document.

Information Security Steering Committee (ISSC) shall review the Bank's Information Security policy annually or upon the occurrence of any significant change within the Bank's operations, that affects the processing, transmission, or storage of information and data.

1.2.4. Policy Dissemination

The information security policy must be published and disseminated to all relevant system users (including vendors, contractors, and business partners).

1.2.5. Risk Assessment

The Bank will carry out an annual risk assessment process that would identify major strategic developments in the industry, emerging threats, & vulnerabilities, to business and IT assets of the Bank and report results in a formal risk assessment document. The formal Risk Assessment should follow some industry-accepted risk assessment methodologies e.g., ISO 27005, NIST SP 800-30, etc.

2. Asset Management Policy

2.1. Introduction

The purpose of this policy is to inform employees of Management's security expectations as it relates to the acquisition, onboarding, maintenance, and decommissioning of the Bank's assets. Assets in this context are Software and Hardware.

2.1.1. Applicability

This policy section applies to all members of staff involved in the procurement, maintenance, and decommissioning of software and hardware assets for the Bank.

2.1.2. Scope

All software and hardware assets currently in use in the Bank and newly acquired assets.

2.2. Software Asset Security

2.2.1. Objective

The objective of this policy is to ensure that, the Bank securely acquires, maintains, and decommissions its software assets.

2.2.2. Policy Statements

2.2.2.1. Asset owners shall appropriately classify all software assets.

- Owners and Custodians shall be determined before the acquisition or development of software.
- Software Owners shall be responsible for the classification of software assets.
- Owners shall be involved in determining the appropriate security controls required for the software.

2.2.2.2. Software custodians shall be responsible for implementing the controls agreed for each software and see to the daily availability of the software.

2.2.2.3. Off-the-shelf software shall be reviewed and certified fit for the intended use before acquisition.

2.2.2.4. Depending on the mode of acquisition, the Bank and the software supplier shall duly sign an acceptable Service Level Agreement(SLA).

2.2.2.5. The Bank shall ensure high availability for all critical software assets.

2.2.2.6. Access to any of the Bank's software assets shall be strictly on a need-to-use basis.

2.2.2.7. The Bank shall enter other legal agreements such as escrow agreements with software manufacturers to ensure the perpetual maintenance of acquired software should the Original Equipment Manufacturer (OEM) cease to be able to continue its operation as a business entity.

2.2.2.8. All internally and third-party developed applications must be thoroughly tested and certified fit for use before deployment to the production environment.

2.2.2.9. The Bank shall put in place appropriate controls to ensure the confidentiality, integrity, and availability of data on all software processing or storing confidential information such as PII (Personally Identifiable Information).

2.2.2.10. The Bank shall put in place appropriate controls to prevent the unauthorized installation of software by users.

2.2.2.11. The Information Technology Group shall securely decommission or retire software assets no longer required for use in the Bank.

2.2.2.12. Members of staff shall not have access to retired software assets unless expressly authorized by Executive Management.

2.2.2.13. Where applicable, the Bank shall notify the software supplier of its intention to retire a software based on the terms agreed upon during the acquisition of the software.

2.3. Hardware Asset Security

2.3.1. Objective

The objective of this policy is to ensure that the Bank securely acquires, maintains, and decommissions its hardware assets.

2.3.2. Policy Statements

2.3.2.1. The Bank shall appropriately tag all hardware assets.

2.3.2.2. The Bank shall appropriately classify all hardware assets.

2.3.2.3. The Bank shall adequately secure and restrict access to all critical assets such as servers.

2.3.2.4. The Bank shall restrict staff from going out of its premises with a hardware asset e.g., server, except laptops. If the need arises, the requesting staff shall obtain authorization from his/her Group Head before exiting the Bank's premises with hardware.

2.3.2.5. Users of the Bank's provisioned PCs and laptops shall be responsible for the security of the asset.

2.3.2.6. The Bank shall define owners and custodians for every piece of hardware.

2.3.2.7. Owners shall be responsible for the classification and security of their assets.

2.3.2.8. Owners shall also be involved in determining the appropriate controls for the security of their assets.

2.3.2.9. Custodians shall be responsible for implementing agreed controls for all assets.

2.3.2.10. Asset custodians shall be responsible for the maintenance of all hardware assets within their custody.

2.3.2.11. Hardware assets shall be securely disposed of when no longer in use.

2.4. Inventory Management

2.4.1. Objective

The objective of this policy is to ensure the Bank has an up-to-date inventory of all its assets; this is important because it gives direction on what to protect and how.

2.4.2. Policy Statements

2.4.2.1. Asset custodians shall maintain an up-to-date inventory of all information assets.

2.4.2.2. Assets, either software or hardware, shall be added to their respective inventories immediately after they are acquired.

2.4.2.3. Assets, either software or hardware, shall be removed from their inventories immediately after decommissioning.

2.4.2.4. Asset owners shall maintain an inventory of their assets.

2.4.2.5. Any hardware deployment or decommissioning shall be reviewed to ensure that all impacts and risks are properly documented.

2.4.2.6. Asset inventories, at minimum, shall contain the following details: asset name, asset owner, asset custodian, asset type/description, asset tag/label, asset location, date purchased, asset model, asset make, asset serial number, and asset lifecycle duration.

2.5. Reference(s)

- Information Management

3. Identity and Access Management Policy

3.1. Introduction

It is the responsibility of the Bank to identify its staff and their actions uniquely, as this is a critical measurement of accountability in today's business world. Considering the Bank's business landscape, it is imperative that the Bank efficiently manages staff identity to mitigate malicious intents such as identity theft and fraud.

3.2. Applicability

This policy is applicable to all staff of PremiumTrust Bank, Third Parties and all information resources used by personnel processing, storing, or transferring PremiumTrust Bank information.

3.3. Scope

All members of staff, Third parties, and all PremiumTrust Bank information processing resources.

3.4. User Profile Management

3.4.1. Objective

The objective of this sub-section is to ensure that only authorized users are given access to the Bank's information, IT systems, and network. This enables the Bank adequately profiles and monitors the activities of its workforce, suppliers, and other stakeholders to prevent unauthorized access, disclosure, and modification of the Bank's data.

3.4.2. Policy Statements

3.4.2.1. Staff's "knowledge of" and "access to" applications shall be strictly based on job function defined for the role established by the Bank.

3.4.2.2. All users must be uniquely identified and authenticated on IT systems that they are authorized to use, in line with their job role.

3.4.2.3. IT Control unit in the Compliance department shall be responsible for Staff Profile Management.

3.4.2.4. The need for privileged user accounts must be strictly limited to those individuals who have an absolute need for such privileges.

3.4.2.5. Elevated permissions may not be assigned to a user's primary account. A separate account must be created for each individual user who has a documented business need for elevated privileges. These accounts should be created with a standard naming convention which will serve to distinguish the account from the user account while at the same time clearly identifying the individual to which the account has been assigned.

3.4.2.6. The use of privileged accounts must be restricted and only used to perform privileged functions, i.e., privileged accounts must not be used for regular user activities.

3.4.2.7. Although privileged access implies a degree of trust in the user being granted such access, core principles such as 'least privilege' and 'need-to-know' should be continually applied.

3.4.2.8. Authorization for the creation of a privileged account must be submitted in writing by the appropriate Data Owner and be approved by the Chief Information Officer and/or the Chief Information Security Officer. Each request for privileged access must include an appropriate justification for the request, as well as an expiration date.

3.4.2.9. All privileged accounts must be secured with a strong, unique password that meets the password strength requirements outlined in the Bank's Password Policy. Privileged users are strictly prohibited from using the same password on their primary account and their privileged account.

3.4.2.10. Passwords for mission-critical systems or very privileged systems shall be written down and securely locked away if there are not more than two persons with access to the system. [This should be sealed and submitted to the Chief Audit Executive and Chief Information Officer, who will keep such in a storage safe requiring dual access (i.e., shared combination lock/keys). Any requests for a password must be duly authorized (written). All accesses will be documented and signed.

3.4.2.11. The use of privileged accounts from physical locations outside of the Bank's Data Center and primary network segments must be secured using multifactor authentication.

3.4.2.12. The risk of abuse associated with using powerful passwords can be minimized through the allocation of equivalent IDs for operational use to individuals to ensure accountability.

3.4.2.13. Staff who are administrators and have other functions shall be given different user IDs for performing these functions.

3.4.2.14. Privileged access rights are to be assigned to different user accounts from those used for day-to-day activities—i.e., employees should not use privileged accounts for their primary job role.

3.4.2.15. Users are to be authenticated using a unique ID and additional authentication for access to the cardholder data environment.

3.4.2.16. Security administration functions shall be audited by independent personnel and exceptions shall be investigated and reported for immediate remediation. Reporting shall be done securely i.e., restricted to staff on a need-to-know basis. Records shall be retained.

3.4.2.17. Each system shall have primary and backup administrators who are able to understand and implement appropriate security procedures.

3.4.2.18. All logical access rights shall be reviewed on a quarterly basis with special attention being given to privileged logical access rights.

3.4.2.19. All logical access activities on critical systems, as defined in risk analysis, shall be logged to an audit trail that is protected from unauthorized logical access.

3.4.2.20. All changes to privileged accounts should be logged and auditable. Audit trails should also contain information on vital activities such as changes to user privileges, use of administrative and other powerful privileges, etc.

3.4.2.21. All privileged user accounts shall be explicitly documented, stating asset type, purpose, expiration, and justification.

3.4.2.22. Accounts shall be deactivated on the date of termination or earlier if required by a risk assessment.

3.4.2.23. De-provisioning tasks shall be concluded in a timely manner to remove any potential for access to systems after leaving.

3.4.2.24. Capability to implement an 'urgent' de-provisioning in emergency situations to immediately mitigate the risk of a rogue employee shall be in place.

3.4.2.25. Files associated with privileged user accounts shall be backed up or otherwise archived before the accounts are removed.

3.5. Logical Access Control

3.5.1. Objective

The objective of this sub-section is to ensure that the Bank grants logical access to all infrastructures on a "need to use" basis to authorized users only.

3.5.2. Policy Statements

3.5.2.1. Provision of logical access to staff shall be strictly based on the role assigned to the user.

3.5.2.2. Logical access to the Bank's network and application shall be strictly on a "need to use" basis.

3.5.2.3. IT Control unit in Compliance shall grant logical access to the network, while IT Audit shall review.

3.5.2.4. Logical access to applications shall be handled by Compliance sequel to approval of requesting officer's Unit and Group Heads and reviewed by IT Audit.

3.5.2.5. Users shall be forced to change their default passwords immediately after user profile creation; users shall also be forced to change passwords, should the need arise.

3.5.2.6. Idle session timeout of 5 minutes shall be set on all systems and critical applications in use within the Bank.

3.5.2.7. Logical access credentials shall be reviewed, and inactive accounts identified; employee accounts without business justification for inactivity shall be disabled immediately.

3.5.2.8. Default credentials on systems and applications shall be disabled; where these are necessary for administration of the systems, a different user shall be created and given the same privileges as the default.

3.5.2.9. A multi-factor authentication mechanism shall be used to authenticate users including third parties on the network and on all payment and critical applications. The multifactor authentication mechanism must incorporate at

least two of the following: 'something you know', such as password; ; 'something you have', such as a token device or smart card; or something you are, such as fingerprints.

3.5.2.10. All remote network access that originates from outside the Bank's network, by employees, administrators and third parties shall require multi-factor authentication.

3.5.2.11. No system, application or database shall be accessed using Group or shared credentials. Group IDs shall only be used in special instances with additional controls implemented to ensure accountability.

3.5.2.12. The use of group and shared IDs and/or passwords or other authentication methods are explicitly prohibited.

3.5.2.13. All users will be assigned a unique ID before allowing them to access system components or cardholder data.

3.5.2.14. The addition, deletion, and modification of user IDs, credentials, and other identifier objects shall be controlled.

3.5.2.15. Manage IDs used by vendors to access, support, or maintain system components via remote access as follows:

- Enabled only during the period needed and disabled when not in use.
- Monitored when in use.

3.5.2.16. Access to all databases must be restricted; only database administrators and other job functions requiring view access can have direct or query access to databases. All other access to databases shall be with an interface or application user.

3.5.2.17. All logical access activities, especially on critical systems must be logged to a Security Information and Event Management System (SIEM).

3.5.2.18. All logical access activities, especially on critical devices shall be reviewed monthly; alert on Indicators of Compromise (IoCs) shall be set on the SIEM and sent to asset custodians as the need arises.

3.5.2.19. Users and Administrators shall not delete application or system logs.

3.5.2.20. The sanction policy will be invoked in cases of attempted unauthorized access.

3.5.2.21. The guidelines below shall be adhered to for password and account management:

- Password length must be at least 8 characters
- Passwords must contain alphanumeric characters and symbols
- Users shall not be able to re-use a password immediately after expiration.
- Password history duration should be set to 12.
- User accounts shall be locked after three (3) failed logon attempt.
- Only the system administrator shall be authorized to enable a locked user account; a formal process for enabling locked accounts should be put in place.
- Passwords shall be stored in an encrypted mode.
- Maximum password age shall be 30 days.
- Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.

3.5.2.22. Intending system users shall be notified that the Bank's information systems are for authorized use only.

3.5.2.23. Users shall not be given a hint of what went wrong during a failed authentication process; a message such as "invalid user credentials" is preferred to "invalid username" or "The password you supplied is not correct".

3.5.2.24. Authorized users on the Bank's network shall ensure the security and protection of their systems from unauthorized access.

3.5.2.25. Authentication mechanisms are assigned to an individual account and not shared among multiple accounts.

3.5.2.26. Physical and/or logical controls are defined to ensure only the intended account can use that mechanism to gain access.

3.5.2.27. Mission critical credentials where applicable shall be 'dualized' and securely locked away; retrieval of the credential must be authorized when required.

3.5.2.28. Logical access rights shall be suspended, revoked, or amended as it applies to any of the scenarios listed below:

- Users on vacation
- Users facing disciplinary action
- Resignation or termination of employment/contract
- Changes in staff responsibility
- Inactive users (at least 90 days)

3.5.2.29. The security requirements of individual applications, information dissemination and contractual and legal requirements shall be considered in designing logical access controls around the information systems.

3.5.2.30. The roles and profiles for each application shall be clearly explained. These will enforce "need to know and need to use" rules and appropriate segregation of duties on the information system.

3.6. Surveillance and Biometric Control

3.6.1. Objective

The objective of this sub-section is to ensure that the Bank monitors activities within its identified critical areas.

3.6.2. Policy Statements

3.6.2.1. Restricted locations such as data centre within the Bank's premises shall be identified.

3.6.2.2. Security personnel shall be positioned at the reception/entrance of all restricted locations.

3.6.2.3. Corporate Services shall review the restricted facility or location to determine the appropriate positioning for adequate CCTV coverage.

3.6.2.4. CCTVs shall be placed at vantage positions that will ensure efficient capture and clarity of footages of events.

3.6.2.5. CCTVs shall be used as a deterrent control where appropriate; however, where expedient, CCTVs shall be hidden from public view.

3.6.2.6. Captured footages must be stored and available for 90days online and a minimum of 12 months offline.

3.6.2.7. Daily review of captured CCTV footages shall be carried out to detect anomalies promptly and proactively.

3.6.2.8. Authorized members of staff shall be authenticated via electronic devices before accessing restricted areas.

3.6.2.9. Authorized personnel shall escort visitors to secure areas. Both shall fill the access register.

3.6.2.10. Logs of activities on the biometric devices shall be fed into a central log management system.

3.6.2.11. IT facilities supporting critical or sensitive business activities shall be located within secure areas.

3.6.2.12. Photographic, video, audio or other recording equipment shall not be allowed into identified restricted areas or facilities of the Bank.

3.6.2.13. Procedures for dealing with physical security incidents shall be established.

3.6.3. Reference(s)

i. Information Management Policy

ii. System Compliance Policy

iii. Cyber Security Policy

4. Network Management Policy

4.1. Introduction

Networks are an integral part of the daily operations of PremiumTrust Bank. Internal networks contain the Bank's vital information and as such, the Bank should deploy appropriate measures to protect these assets. Furthermore, interaction with external networks such as the Internet and other third-party networks such as Interswitch, introduces the risk of compromising the Bank's information resources' confidentiality, integrity, and availability.

4.2. Applicability

This policy is applicable to the Bank's Head Office, branches, employees (including

temporary staff), contractors, consultants, third parties and service providers utilizing the Bank's network resources.

4.3. Scope

All personnel defined under applicability above, network devices, and all computing equipment used on the Bank's network.

4.4. Network Perimeter Security

4.4.1. Objective

The objective of this sub-section is to ensure that the Bank permits only authorized traffic in and out of its network.

4.4.2. Policy Statements

4.4.2.1. Formal procedures shall exist to approve any service request through the Bank's network perimeter devices; every service request shall have an approved business objective.

4.4.2.2. A risk-based approval process shall exist to identify additional risks introduced to the business by the service.

4.4.2.3. The internal network shall be efficiently and effectively segmented.

4.4.2.4. The internal network shall be separated from the external network by a network security perimeter. This separation shall be established through a secure Demilitarized Zone (DMZ).

4.4.2.5. Network perimeters shall be configured by default to prohibit all that is not explicitly allowed; permitted connections and protocols through the perimeter shall be explicitly defined. Any connection or protocol not explicitly defined and permitted shall be prohibited by the network perimeter.

4.4.2.6. Network perimeters shall be monitored for policy violations; the configuration of a network perimeter shall be such that it is able to detect unauthorized access attempts. Intrusion detection measures and/or alerting mechanisms shall be employed to facilitate this service. At predefined thresholds, preventive controls shall be activated. This will include a denial of access and appropriate logging of access violation attempts.

4.4.2.7. Secret and confidential data shall be encrypted when sent over external networks. External networks refer to networks that are not directly managed by PremiumTrust Bank and include Internet, service provider networks, networks of partner banks, and correspondent organizations.

4.4.2.8. All new IT facilities shall be technically approved and authorized before installation; new IT facilities shall require Management approval to ensure that the installation is for a clear business purpose, will provide adequate security, and will not adversely affect the security of the existing infrastructure.

4.5. Internal Network Security

4.5.1. Objective

The objective of this sub-section is to ensure that the Bank protects its internal network from malicious unauthorized access and its succeeding implications such as information confidentiality breach, data exfiltration, malware spread, and fraud.

4.5.2. Policy Statements

4.5.2.1. Configuration items on network resources shall be backed-up and restored on a regular basis in accordance with the Business Continuity Management Policy.

4.5.2.2. All information traversing network resources shall be appropriately safeguarded in accordance with the Information Classification Policy.

4.5.2.3. A log of all operational network activities shall be maintained.

4.5.2.4. Information and Cyber Security and Technology Groups shall review the network activity logs and generate the report as appropriate.

4.5.2.5. User passwords shall be encrypted when transmitted over internal networks. Other data sent over internal networks shall be encrypted based on risk assessment.

4.5.2.6. The Bank shall maintain an Internal Certificate Authority (CA) infrastructure to secure non-customer-facing web applications.

4.5.2.7. The Internal Certificate Authority shall be deployed as follows:

- The CA system shall be installed and managed securely with appropriate physical and logical controls.
- The Certifying Authority shall keep a secure backup of its private keys. Backed-up keys must be stored in an encrypted format and protected from environmental threats. A copy of the backed-up keys shall be stored in an offsite location for protection against disasters.
- There shall be a well-defined and documented procedure for issuance of certificates including user request, user credential verification, certificate approval, and user undertaking.
- The administrator of the CA infrastructure shall generate the required user key pairs. It shall be ensured that no copy of the user's private key is retained by CA to avoid the risk of repudiation.
- To reduce the likelihood of compromise, certificates shall have a defined activation and deactivation date, so that they can be used only for a limited period. The Bank shall decide the validity period of the user certificate. If the CA's private key is compromised, users shall be warned about a key compromise.

- All affected user certificates should be revoked thereafter.
- Change CA private key and reissue user certificates.
- For the protocol in use to only support secure versions and configurations (that insecure versions or configurations are not supported).

4.6. Network Device Hardening

4.6.1. Objective

The objective of this sub-section is to ensure that the Bank securely configures its network devices prior to usage on a live environment.

4.6.2. Policy Statements

4.6.2.1. Access to network resources shall be managed in accordance with the Identity Management Policy.

4.6.2.2. All changes to network resources shall be in accordance with the Change Control Policy.

4.6.2.3. External facilities shall be managed with the same level of protection as onsite facilities housing the same category of information resources in accordance with the Physical and Environmental Policy and Third-Party Access Policy.

4.6.2.4. The Bank's network resources shall be protected against malicious program code in accordance with the Bank's Anti-malware Management policy.

4.6.2.5. Information Technology shall delete all default accounts on all network devices prior to usage on the live environment.

4.6.2.6. Where applicable, Information Technology shall disable all unused services on all network devices.

4.6.2.7. Information Technology shall adequately patch all network devices.

4.6.2.8. Information Technology shall ensure that all network devices are configured to send logs to the Bank's Security Information and Event Management (SIEM) Tool.

4.6.2.9. Information Technology shall configure CPU utilization threshold on all network devices.

4.6.2.10. Information Technology shall configure account lockout feature for multiple failed logons attempts on all network devices in line with the policy

4.6.2.11. Information Technology shall securely configure NTP communications on all network devices.

4.6.2.12. Information Technology shall securely deploy SNMP on all network devices; the use of unsupported and insecure versions of SNMP is prohibited.

4.7. Third-Party Network Integration

4.7.1. Objective

The objective of this sub-section is to ensure that, the Bank institutes a process that will ensure effective and adequate management of Third-Party Integrations to the Bank.

4.7.2. Policy Statements

4.7.2.1. Remote access to the Bank's network resources shall only be granted through an authorized remote access process.

4.7.2.2. The Bank shall use PKI for communicating with external entities where high-value transactions are conducted and where there is a risk of legal or contractual liability.

4.7.2.3. While evaluating PKI as a solution for communicating with external entities, the ability of the external party to ensure the security of the certificate shall be considered.

4.7.2.4. Remote access shall be granted for business purposes only.

4.7.2.5. The following category of users shall be considered for remote access; permanent staff, temporary staff, and third parties who require access to perform essential functions when not at their normal place of work, such as after-business hours support. The benefits and risk considerations shall be evaluated in the procedure for granting remote access to users. Only authorized users at the remote site shall utilize remote access facilities.

4.7.2.6. All remote access connections shall be authorized; procedures and processes for remote access authorization shall be established. Remote access shall only be permitted upon authorization from the Information Custodian, CIO, and the CISO.

4.7.2.7. A register of all authorized remote access users shall be maintained; the register of authorized remote access users, as well as the access levels provided, shall be reviewed regularly to confirm that there is still a valid business requirement. The register of remote access shall also be reviewed regularly to identify expired or unnecessary privileges.

4.7.2.8. Remote access shall be governed by a formal process; remote access by users shall be governed by signed, formal agreements between the Bank and the user, which:

- Clearly define the responsibilities of remote users.
- Outline a code of conduct to which remote users shall adhere.
- Require the remote user to comply with any necessary security policy, standards, and procedures.
- Require the remote user to agree that only authorized software is installed on the electronic device used to connect to the Bank's network.

4.7.2.9. Remote access shall only be provided via the Bank's dedicated and approved remote access facilities; all remote access connections shall be made via the Bank's approved remote access infrastructure.

4.7.2.10. The connection capabilities of remote access users shall be restricted to the approved requirements; remote users shall be restricted to the minimum and approved functions necessary for the business process.

4.7.2.11. Remote access users shall be identified and authenticated. The level of identification and authentication shall be based on the classification of information being accessed; remote access authentication shall be performed using authentication mechanisms based on the classification of the information being accessed.

4.7.2.12. Remote access server shall log all connections. The remote access server shall log both successful and unsuccessful connections. These logs shall be in a format that will facilitate effective analysis of the results.

4.7.2.13. Successful and unsuccessful remote access connections and sessions shall be reviewed and reported. Successful sessions shall be analysed for trends or patterns, which may indicate misuse of the remote access facilities.

4.7.2.14. Unauthorized or unsuccessful access attempts and/or exceptions shall be reported as required by the Bank's Incident Management Procedures.

4.7.2.15. Remote access users shall be educated on the additional security requirements for the protection of equipment, software, and information. Users shall be made aware of the necessary protection measures for remote access, for example, all information necessary for remote connections shall be considered confidential. Users issued with such shall not disclose it to any other person, either internal or external to the Bank. Any strong authentication tools shall also be protected.

4.7.2.16. Remote access users shall not concurrently connect to the Bank's network and another network unless in compliance with the Bank's Third-Party Access Policy; users shall ensure that when connecting to the Bank's network, all other connections are disabled. The exception being when the other connection has been authorized in compliance with the Bank's Third-Party Access Policy.

4.7.2.17. Anti-malware shall be installed and updated on all remote access clients, and the anti-malware on remote access connections shall be kept up to date.

4.7.2.18. Remote access privileges shall be reviewed and removed when no longer required; remote access shall be granted for a specified period. Authorization for remote access shall be revoked when:

- the specified period has elapsed,
- the connection is no longer required,
- employment has been terminated,
- remote user is deemed to be in breach of the Remote Access Agreement
- remote user's account is inactive.

4.7.2.19. All users of off-site devices shall comply with all security policy requirements stipulated by the Bank, in addition to any specific security standards and procedures which may be in place. Software configuration shall comply with the Bank's security standards.

4.7.2.20. All remote access connections (through the Bank or Third-Party electronic devices) shall be via secured processes in compliance with the Bank's Remote Access Standards.

4.7.2.21. Passwords shall be encrypted during network transmission. However, if not possible, an assessment of the implications shall be undertaken.

4.7.2.22. Logical Access controls shall have multiple authentication mechanisms e.g., token/OTP, etc. Remote access control mechanisms shall be separate and additional to internal network and application access mechanisms.

4.7.2.23. All remote access users shall comply with the Bank's Identity and Access Management Policy.

4.7.2.24. All information traversing remote access connections shall be protected according to the Bank's Information Management Policy; Information traversing remote access connections may be sensitive and should be treated accordingly. Users of remote access equipment shall be provided with encryption facilities if they are required to hold or transmit confidential information while off-site.

4.7.2.25. When resetting a remote user's credentials, the authenticity of the remote user shall be determined. This shall be through a formal approval process.

4.7.2.26. Third-Party connections and security considerations for each type of connection shall be defined as follows:

- The types of connections and strengths of the controls (e.g. monitoring and logging) for each type of connection shall be defined.
- The level of protection required shall be determined based on a risk assessment of the information to be accessed and in some cases, may require cryptography-based solutions based on Information Management Policy and/or the use of non-disclosure agreements. Logging and monitoring of connections shall be performed where appropriate.
- Transmission of information classified as secret or confidential shall be encrypted.

- Information classified as a secret or confidential shall be encrypted at rest.
- Encryption mechanisms shall be subjected to an approval procedure that considers the type and volume of information being transmitted.
- Encryption mechanisms shall be re-evaluated for appropriateness every 12 months.
- Assignment and distribution of public/private keys shall be via a documented procedure.
- The procedures shall ensure that the same cryptographic key is not used for different communicating pairs.
- Encryption keys shall be changed from default values at the time of equipment installation.
- Encryption keys shall be set up such that at least two people are required to make key changes and control physical keys for encryption hardware.

4.7.2.27. All Third-Party Connection requests shall be submitted and approved based on business needs and risk analysis results.

- Group Head of requesting Officer, CIO, CISO, and other relevant stakeholders shall be responsible for originating and approving all requests for Third-Party Access.
- Approval shall be given for Third-Party Access if the request is made by authorized personnel and subject to the fulfilment of all other conditions.
- A risk assessment shall be performed to identify the security implications and adequacy of controls needed to reduce risks to an acceptable level.

- The assessment considers the type of connection, the value of the information, the Third Party's security measures, and the implications for the Bank's IT infrastructure.
- Where access to an application is required, written authorization from the Information Owner and Custodian shall be obtained.

4.7.2.28. Business and technical risk analysis shall be performed for all Third-Party connections.

4.7.2.29. The authorization of Third-Party connections shall consider the classification of the information being accessed.

4.7.2.30. Security software shall be used to protect Electronic Data Interchange (EDI) transactions, programs, and files from unauthorized access.

4.7.2.31. Measures shall be taken to safeguard Virtual Private Network (VPN) connections.

- All VPN connections security controls shall have multi-factor authentication mechanisms e.g., token, OTP etc.
- Process for VPN security connections shall produce full audit trail information.
- All audit trails shall be monitored daily for unauthorized access attempts.
- Unauthorized access attempts shall be investigated promptly.

4.7.2.32. The least privilege principle shall be applied to any Third-Party connection; The least privilege principle implies that third parties shall be restricted to the minimum services and functions necessary for the business process.

4.7.2.33. Physical access to information resources by third parties shall be restricted; Third parties shall only have access to designated areas, as determined and approved by the CISO based on business requirements.

4.7.2.34. All Third-Party agreements shall be formalized in a contract; Third-Party Access shall be governed by signed, formal agreements. Third-Party Access shall not be allowed without these agreements. The following should be considered:

- Third-Party users and any subcontractor that is used by the Third Party, shall comply with all applicable PremiumTrust Bank's information security policies, standards, and procedures e.g., controls to ensure protection against malicious software and escalation procedure for problem management:
- Responsibilities of Third-Party users
- Contract expiry dates
- Code of conduct to which Third-Party users will adhere
- Available services and respective access levels
- List of authorized users
- The right to monitor and revoke users
- Respective liabilities of parties to the agreement
- Specification of intellectual property rights
- Legal responsibilities
- Return of assets and information measures
- The right of PremiumTrust Bank to audit the Third Party's information systems environment.

- Relevant escape clauses; and
- Confidentiality agreements for all Third-Party connections.

These agreements shall be reviewed regularly to confirm that there is still a valid business requirement for existing Third-Party access.

4.7.2.35. Authorization for Third-Party shall be revoked immediately the Third-Party service is no longer required or if a Third-Party is deemed to be in breach of the Third-Party agreement.

4.7.2.36. If cardholder data is shared with service providers, then contractually the following shall be required:

- Service providers must adhere to the PremiumTrust Bank's compliance requirements.
- Agreement that includes an acknowledgement that the service provider is responsible for the security of cardholder data the provider possesses.

4.7.2.37. Users shall be educated on the security conditions imposed by Third-Party providers and the concerned Unit Head/Group Head shall sign an undertaking that they understand the risks.v

4.7.2.38. A record of all authorized Third-Party users and their access rights shall be maintained and reviewed at least biannually by the Information & Cyber Security group to ascertain the existence of valid business justification for all existing Third-Party users, determine inactive users and users with expired privileges. The Information & Cyber Security group shall maintain a register of all Third Parties requests. The register is to include the duration and specific periods when access is permitted, together with a log of all access.

4.8. Cryptography Control

4.8.1. Objective

The objective of this sub-section is to ensure that cryptographic controls utilized by the Bank conforms to current standards and can ensure the confidentiality of the data being protected.

4.8.2. Policy Statements

This policy document addresses PremiumTrust Bank's Key Management Requirements and Card Data Encryption.

4.8.2.1. Card data whenever it occurs in conjunction with PAN must be encrypted. This is applicable to all data stored including data on database, portable digital media, backup media, in logs, and data received from or stored by wireless networks.

4.8.2.2. A list of roles that need access to display of full PAN is documented, together with a legitimate business need for each role to have such access.

4.8.2.3. PAN must be masked when displayed such that only personnel with a legitimate business need can see the full PAN.

4.8.2.4. All other roles not specifically authorized to see the full PAN must only see masked PANs.

4.8.2.5. Encryption of card data will be carried out using Symmetric Key Encryption: AES 256 bits, or Asymmetric Key Encryption: RSA 2048 Bits, Diffie Hellman 2048 Bits, El Gamal 2048 Bits

4.8.2.6. The responsible officer shall consider algorithm performance when deciding on encryption standards to be used for data security; Advanced Encryption

Standard (AES) has been proven to have better algorithm performance compared to Triple Data Encryption Algorithm (TDEA).

4.8.2.7. Where Asymmetric Key Encryption Algorithms are used, the responsible officers shall put controls in place to ensure the non-disclosure of the private key.

4.8.2.8. The use of discontinued encryption standards such as Data Encryption Standard (DES) is prohibited.

4.8.2.9. The minimum account information that must be rendered unreadable is the PAN.

4.8.2.10. Encryption keys will be stored in a location separate from the encrypted data.

4.8.2.11. Cardholder data on removable media will be encrypted wherever stored.

4.8.2.12. Native file system disk encryption will not be used to encrypt card data.

4.8.2.13. Encryption keys used for encryption of cardholder data will be protected against both disclosure and misuse by:

- Restricting access to keys to the fewest number of custodians necessary
- Secure storage of keys in the fewest possible locations and forms

4.8.2.14. Key management processes and procedures for keys used for encryption of cardholder data will be documented and implemented for:

- Generation of strong keys
- Secure key distribution
- Secure key storage
- Periodic key changes (at least Annually)
- Destruction of old keys

- Split knowledge and establishment of dual control of keys (so that it requires two or three people, each knowing only their part of the key, to reconstruct the whole key
- Prevention of unauthorized substitution of keys
- Replacement of known or suspected compromised keys
- Revocation of old or invalid keys

4.8.2.15. Key custodians to sign a form stating that they understand and accept their key-custodian responsibilities.

4.8.2.16. Users shall ensure the following in the use of encryption keys:

- Users should ensure that their private keys are kept strictly confidential and not available to anyone else including the Certifying Authority.
- Users should safeguard the private key by locking with password and/or by storing on media like smart card that is always under the custody of the user.
- If there is a compromise of private key or if the key is unavailable (because of damage to key storage media) it should be immediately reported to the Registration Authority/CA.
- Users should maintain an updated copy of certificate revocation list to ensure that expired or compromised certificates are not used in transactions.
- Users should ensure that certificate is renewed before expiry.

4.8.2.17. The Bank would take the following into consideration when acquiring the service of a Certifying Authority (CA):

- **Trust** – Is the CA organized, controlled, and regulated in such a way that its operations can be relied upon and checked?
- **Accreditation** - Is the CA accredited by the recognized national, regional, and international groups?
- **Compliance** – Is the CA operating in compliance with accepted industry standards and all relevant regulations?
- **Contract** – Is there a legally binding contract in place covering the provisions of the service and addressing all the issues?
- **Liability** - Is there a clear understanding as to the issues of liability? Under what circumstances is the CA liable for damages? Is the liability adequate considering PremiumTrust Bank's exposure? Does the CA have sufficient resources to meet its potential liabilities?
- **Security Policy** – Does the CA have a security policy covering technical and administrative requirements?
- When using the services of an external CA, PremiumTrust Bank can act as Registration Authority (RA) for its employees. RA is responsible for validating the credentials of Bank employees seeking digital certificates and revocation reporting.

1.1. **Reference(s)**

i. Asset Management Policy

ii. Cyber security Policy

iii. Supply Management Policy

5. Application Management Policy

5.1. Introduction

Applications are essential components of the Bank's service delivery infrastructure. It is paramount that the Bank's internally and externally accessible application are securely implemented as applications represent a major attack surface for threat actors.

5.2. Applicability

This policy is applicable to all staff involved in application development or purchase of off-shelf applications for the use of the Bank. It also applies to all stakeholders involved in application development, maintenance, and testing.

5.3. Scope

All applications developed and bought off-the-shelf for use in the Bank are subject to the requirements of this policy.

5.4. Application Development Security Control

5.4.1. Objective

The objective of this sub-section is to ensure that the Bank's applications are securely developed and free of any of the Open Web Application Security Project (OWASP) Top 10 vulnerabilities and other critical application vulnerabilities.

5.4.2. Policy Statements

5.4.2.1. The Bank shall adopt a Software Development Life Cycle/Methodology; the adopted software development methodology shall apply to all in-house-developed applications.

5.4.2.2. All applications developed within the Bank shall undergo a risk assessment exercise prior to the commencement of the development process; the Business Requirement Document (BRD) or Standard Work Request (SWR) shall be

considered as source documents for the risk assessment, stakeholders such as the business and Information Technology team shall be engaged as well.

5.4.2.3. The Bank shall have a separate environment from the production environment for application development and testing.

5.4.2.4. The following Software Development Life Cycle (SDLC) stages shall be incorporated into the SDLC process adopted by the Bank:

- Requirement Gathering/Business Request Documentation
- Business request review
- Risk assessment
- Application development
- Application security review
- User Acceptance Test
- Deployment and Post Deployment review

5.4.2.5. A unit independent of the development team shall carry out application code review and certify that, application codes are defect-free and comply with the Bank's coding or adopted coding standard.

5.4.2.6. The Information and Cyber Security group shall test internally developed application and confirm the non-susceptibility of applications to the OWASP standard and other critical vulnerabilities prior to approving the project for the next milestone.

5.4.2.7. The Bank shall not use critical live data such as PAN and CVV on the test environment.

5.4.2.8. The Bank shall delete test data prior to migration of new or changed application to live environment.

5.5. Third-Party Application Integration Control

5.5.1. Objective

The objective of this sub-section is to ensure that the Bank assesses and can ascertain that a Third-Party application is fit for use and secure prior to integration of such an application into its network.

5.5.2. Policy Statements

5.5.2.1. The Bank shall always ensure the highest possible level of security when integrating with Third Parties; the Bank shall not relax its security controls for a Third-Party integration unless approved by the Chief Information Officer and the Business Group Head, after a risk assessment of the relaxation has been done by the Information & Cyber Security Group.

5.5.2.2. The bank shall maintain a written agreement that includes an acknowledgement that the service providers will maintain all applicable PCI DSS requirements to the extent the service provider handles, has access to, or otherwise stores, processes, or transmits the customer's cardholder data or sensitive authentication data, or manages the customer's cardholder data environment on behalf of a customer.

5.5.2.3. The bank shall maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.

5.5.2.4. Where possible and applicable, the Bank shall conduct a code review of Third-Party Applications before integrating such applications into the Bank's network.

5.5.2.5. For Third-Party integrations requiring VPN connections, the Bank shall implement the connection using the strongest encryption standard possible for such

connections; the Bank shall not use weak encryption standards no longer recommended for use.

5.5.2.6. Where possible and applicable, the Bank would carry out penetration testing on Third-Party Applications and certify that the application is fit for use prior to live deployment. However, where there is no internal competency, a Third-Party shall be engaged to carry out the test.

5.5.2.7. Executive Management approval shall be obtained prior to conducting a penetration test.

5.5.2.8. The Information and Cyber Security Group shall conduct vulnerability assessment on all Third- Party Applications prior to live deployment.

5.5.2.9. Connected entity requirements: all processors and service providers must maintain and implement policies and procedures to manage connected entities, to include the following:

- Maintain list of connected entities.
- Ensure proper due diligence is conducted prior to connecting an entity.
- Ensure the entity is PCI DSS compliant.
- Connect and disconnect entities by following an established process.

The following are additional requirements to ensure safe integration:

1. **Segmentation of third parties:** Business units shall maintain the type and criticality of third- party services. These shall be sorted into risk-based tiers for due diligence and refreshed frequently – Low risk, Medium risk, and High risk. Further due diligence shall not be required for low-risk third parties.
2. **Scope of Service:** Relevant controls shall be assigned based on the data and systems accessed by each third party. At onboarding, the responsible

business/service owner shall ensure that contract documents are adequately executed with the relevant clauses where applicable (e.g., the right to audit clause). The Bank's Legal team shall ratify this.

3. **Assessment:** In collaboration with Business units, the Information &Cyber Security Group shall assess the inherent risk in each relationship and criticality of service. This shall be done annually or after a significant change. The Information & Cyber Security Group shall assess the effectiveness of third-party controls. Questionnaire responses and document artefacts shall serve as evidence for the third-party risk assessment.
4. **Implementation:** Information Technology Group shall implement all policy requirements after Change Management approval.
5. **Remediation:** Ineffective controls shall be identified and remediated.
6. **Monitoring:** Information and Cyber Security Group shall regularly review connections and APIs of third-party relationships to ensure that the Bank is not at any time exposed to cybersecurity risks.
7. **Reporting**: Information and Cyber Security Group shall provide a periodic report of third-party service providers' risk assessment.

5.6. Web Application Security

5.6.1. Objective

The objective of this sub-section is to ensure that the Bank's web applications are securely developed and free of any of the OWASP Top 10 vulnerabilities and other critical application vulnerabilities.

5.6.2. Policy Statements

5.6.2.1. The Information and Cyber Security Group shall develop baseline configurations for all the web server types in use in the Bank.

5.6.2.2. The Bank shall deploy a Web Application Firewall (WAF) to protect all internet/external facing web applications.

5.6.2.3. The Information and Cyber Security Group shall certify that no internally developed web application is susceptible to any of the OWASP Top 10 vulnerabilities and other critical vulnerabilities.

5.6.2.4. An independent code review on internally developed web applications, and certify that, the codes are defect-free and comply with the Bank's adopted coding standards.

5.6.2.5. The Bank shall encrypt every communication with its web applications, especially the internet facing web applications.

5.6.2.6. The Bank shall carry out at least a quarterly scan of its entire critical internet facing webservers; the Information and Cyber Security Group must obtain an Approved Scan Report from the Approved Scanning Vendor (ASV) adopted by the Bank.

5.6.2.7. For off-the-shelf web applications, the Information and Cyber Security Group shall conduct an assessment on the application and get a statement of assurance (document) from the vendor over the security of the application.

5.6.2.8. Checks shall be performed to detect out of range values, invalid characters, incomplete data, exceeding upper or lower data limits, unauthorized and inconsistent control.

5.7. Secure Coding and Review

5.7.1. Objective

The objective of this sub-section is to ensure that the Bank validates that its applications are securely developed, and only authorized users have access to application source codes.

5.7.2. Policy Statements

5.7.2.1. The Bank shall develop its own or adopt a secure coding standard.

5.7.2.2. The Bank's Application development team shall develop applications in line with the Bank's adopted coding standard.

5.7.2.3. Training in secure coding techniques is required for developers and that training is based on Industry best practice.

5.7.2.4. An Internal Quality Assurance Team shall execute code review on all internally developed source codes and certify that, such codes are defect-free and comply with the Bank's adopted coding standard.

5.7.2.5. All custom application code changes must be reviewed (using either manual or automated processes) as follows:

- Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code review techniques and secure coding practices.
- Code reviews ensure code is developed according to secure coding guidelines (see PCI DSS Requirement 6.5).
- Appropriate corrections are implemented prior to release.

- Code-review results are reviewed and approved by management prior to release.

5.7.2.6. Pre-production and/or custom application accounts, user IDs and/or passwords are removed before an application goes into production or is released to customers.

5.7.2.7. The Bank shall explicitly restrict access to application source codes; only authorized users can have access to source codes.

5.7.2.8. The Bank shall explicitly deny access to source codes of all applications on the production/live environment.

5.7.2.9. Source codes shall be stored in restricted environments with appropriate privileges to authorized users.

5.7.2.10. A formal approval process shall be in place for source code retrieval.

5.7.2.11. Download, copying and printing of source codes on unauthorized devices shall be prohibited.

5.7.2.12. Modifications to existing application source codes shall comply with the Bank's Change Management Policy.

5.7.3. Reference(s)

i. Identity Management Policy

ii. Information Management Policy

iii. Change Management Policy

6. System Compliance Policy

6.1. Introduction

Systems are critical information-processing facilities that enhance service delivery to our

customers. Taking into consideration the criticality of information processed and transmitted by these systems, it is important to ensure the fortification of these systems against known threats that can compromise the confidentiality, availability and integrity of the systems and the information processed and stored on these systems.

6.2. Applicability

This policy section is applicable to all Systems Administrators in the Bank and all members of staff. Administrators involved in the setup of new PCs, laptops and servers should ensure adherence to the requirements of this policy. All third parties connecting to the Bank's network are also expected to adhere to the requirement of this policy. This policy also applies to mobile devices (personal or "Bank-provisioned") that are used for processing, transmission and storing the Bank's information.

6.3. Scope

All systems, servers and Third-Party systems connecting to the Bank's network constitute the scope of this policy.

6.4. Desktop Hardening

6.4.1. Objective

The objective of this sub-section is to ensure that all systems within the enterprise adhere to the minimum-security requirements for connecting to the Bank's network.

6.4.2. Policy Statement

6.4.2.1. A baseline configuration checklist containing 'business-approved applications' to be installed and needed services on PCs and laptops shall be developed.

6.4.2.2. All systems in use within the Bank must be configured with the baseline configuration checklist before handing over systems for staff use.

6.4.2.3. Staff shall not be able to initiate Remote Desktop Connection (RDC) to other staff systems unless this is required for the staff's day-to-day activities.

6.4.2.4. All system shall be installed with the latest version of the anti-malware software in use in the Bank during system configuration.

6.4.2.5. Default accounts shall be disabled on all systems.

6.4.2.6. Access to systems shall be explicitly denied unless user is successfully authenticated.

6.4.2.7. Data Loss Protection shall be implemented on all systems in use within the Bank.

6.4.2.8. Operating System and application patches/updates shall be tested and deployed as required based on patch schedule.

6.5. Server Hardening

6.5.1. Objective

The objective of this sub-section is to ensure that all servers meet the minimum-security requirements specified and approved by the Bank prior to utilization on production or test environment.

6.5.2. Policy Statements

6.5.2.1. Baseline Configuration Checklist shall be developed for all server Operating Systems in use within the Bank (Windows, Linux, UNIX, etc).

6.5.2.2. Configuration baselines shall be dependent on the function of the server; bearing in mind that, different configuration applies to different server types e.g., Configuration for a Webserver shall differ from that of a database server.

6.5.2.3. The latest stable version of Operating System (OS) shall be installed on servers when configuring the server for use.

6.5.2.4. Applicable baseline configuration must be implemented on server while setting up the server for use.

6.5.2.5. Default accounts shall be disabled on all servers.

6.5.2.6. Logical access to servers shall be explicitly denied except for approved system administrators.

6.5.2.7. Only required services for the functioning and administration of a server shall be enabled on the server; it should be noted that services to be enabled would differ for different servers. For example, a Mail server and a Web server would not require the same set of services for proper functioning and administration.

6.5.2.8. Operating System and application patches/updates shall be tested and deployed as required based on patch schedule.

6.6. Anti-malware Management

6.6.1. Objective

The objective of this sub-section is to provide guidance on the deployment, maintenance, and utilization of the Bank's approved anti-malware solution.

6.6.2. Policy Statements

6.6.2.1. Only the Bank's approved anti-malware software shall be installed and used on all systems within the Bank.

6.6.2.2. The latest version of the approved anti-malware software in use in the Bank shall be installed on new systems as part of the system configuration process before the system is handed over to the user.

6.6.2.3. All systems in use shall always have active and up-to-date anti-malware software.

6.6.2.4. The approved anti-malware must be able to carry out at the minimum the under-listed:

- Identification and protection of all systems from known malware infections.
- Automatic scanning of removable media as soon as, they are plugged to a system.
- Automatic scanning and identification of malicious contents in mails and mail attachments prior to file download.
- Capable of executing actions such as sandboxing and deleting identified malicious files/contents.

6.6.2.5. Anti-malware software and its definitions shall be automatically updated as the need arises on PCs, Laptops and Servers.

6.6.2.6. Staff shall be educated on how to validate the version of the anti-malware software on their systems and escalate out-of-date anti-malware version to Information Technology Service desk.

6.6.2.7. Periodic automated scans of desktops, laptops, and servers in use in the Bank shall be conducted using the Bank's approved anti-malware software.

6.6.2.8. The anti-malware software shall be centrally administered and controlled on all systems daily.

6.6.2.9. The Bank's approved anti-malware software must be capable of generating and retaining audit logs for at least 3 months.

6.6.2.10. The Information and Cyber Security Group shall ensure that connecting Third-Party users have an antimalware software installed on their systems.

6.6.2.11. The Bank shall install its approved antimalware software on the Third-Party user's system provided the user does not have an antimalware software installed on his/her system for the duration of access.

6.6.2.12. Supported anti-virus software must be installed and updated at regular intervals.

6.6.2.13. Anti-virus software and virus pattern files or definitions must be kept up to date.

6.6.2.14. Virus-infected computers must be removed from the network until they are verified as virus- free.

6.6.2.15. All software to be deployed/ installed on the Bank'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.

6.6.2.16. Antivirus software shall be actively running and must not be disabled or altered by users.

6.6.2.17. Antivirus software shall be capable of protecting against, detecting and removing all types of malicious software.

6.6.2.18. It is required that the antivirus software is kept up to date, and a version review conducted quarterly.

6.6.2.19. The antivirus database must be set to automatically update.

6.6.2.20. Periodic antivirus scans are required in accordance with regulatory and information security requirements.

6.6.2.21. In the event of malware causing loss, an investigation must be conducted, where forensic methods may be used to satisfy legal and regulatory requirements.

6.6.2.22. Antivirus logs must be retained for at least one year.

6.6.2.23. Processes must be in place to restore the last three months of logs for forensic analysis.

6.7. System Endpoint Management

6.7.1. Objective

The purpose of this policy is to minimize data loss via system sharing services or hardware.

6.7.2. Policy Statements

6.7.2.1. The Bank shall implement controls that would prevent data/information loss due to user activities

6.7.2.2. The Bank shall implement the following guidelines:

- USB ports should be explicitly disabled on all systems
- CD Drives should be disabled on all systems
- Appropriate controls shall be implemented to ensure only authorized attachments shall be allowed for all outgoing mails from cloud infrastructure. Attachment limit size of 20MegaBytes should be set for all outgoing mails (mails leaving the Bank's network) from on-premises email servers.

6.7.2.3. Access to information classified as confidential or secret on cloud environment should be available to only authorized users.

6.7.2.4.

6.8. Mobile Device Management

6.8.1. Objective

The objective of this sub-section is to provide guidance on the secure usage of personal or provisioned mobile devices as it relates to the processing and storage of the Bank's information.

6.8.2. Policy Statements

6.8.2.1. Mobile/Portable information assets must be:

i. Physically protected against loss, theft, damage, and unauthorized access - they must not be left unattended in public areas, unlocked offices, vehicles, hotel rooms, homes etc. without being physically secured e.g., using an approved security cable lock, safe or at the very least tucked away out of sight; and

ii. Logically protected against malware, unauthorized access and unauthorized configuration changes using security products approved for this purpose by Information and Cyber Security Group.

6.8.2.2. Sensitive personal or proprietary data stored on portable information devices and media must be encrypted using suitable products and procedures approved by Information and Cyber Security Group.

6.8.2.3. Corporate IT equipment, including portable devices and media, must only be used by authorized users for legitimate business purposes.

6.8.2.4. Unauthorized software must not be loaded onto corporate IT equipment, including portable devices and media.

6.8.2.5. Employees must not interfere with or disable security controls on corporate IT devices, including portable devices and media.

6.8.2.6. Before corporate information assets, including portable devices and media, are disposed of, or allocated to other users, residual information must be physically destroyed or securely erased using procedures approved for this purpose by Information and Cyber Security Group.

6.8.2.7. Employees must report security incidents and near misses, including those involving portable information assets in line with Incident Management Policy.

6.8.2.8. Employees that process, transmit or store the Bank's information on their mobile device or a Bank-provisioned mobile device shall logically protect the mobile device from unauthorized access.

6.8.2.9. Employees involved in mobile computing shall ensure the physical security of the mobile device.

6.8.2.10. All employees processing the Bank's information on their personal mobile devices shall ensure the installation and continuous update of an antimalware software on their mobile device.

6.8.2.11. Employees shall not copy, transfer, make a screenshot or convey any information pertaining to the bank from their mobile devices by any software, or means for unapproved use and without the consent of Information and Cyber Security Group.

6.8.2.12. Employees shall where applicable deploy the use of Rights Management Services to control access and use of information transmitted to end users or recipients in accordance with ISO policies

6.8.3. Reference(s)

i. Network Management Policy

ii. Identity and Access Management Policy

iii. Information Management Policy

7. Information Management Policy

7.1. Introduction

Customers' information just like business-critical documents are vital to the existence of the organization as a going-concern. With the increasing and sophisticated attack patterns targeted at financial institutions in today's business world, it is important for the Bank to manage its information assets effectively.

Implementing an effective information management process would help ensure the security of the Bank's information.

7.2. Applicability

This policy is applicable to all staff of PremiumTrust Bank and all third Parties that access, process, transfer, and store PremiumTrust bank's information.

7.3. Scope

All PremiumTrust Bank's information, physical and electronic.

7.4. Information Classification

7.4.1. Objective

The objective of this sub-section is to ensure that the Bank accurately classifies its information; this will assist in ensuring the implementation of appropriate security measures on classified information.

7.4.2. Policy Statements

7.4.2.1. The Bank shall classify its information according to the following criteria:

- **Public:** Information generally available for public use without restriction.
- **Internal Use:** Use restricted just within the organization.

- **Confidential:** These are business critical information than can be available electronically, orally or in print. Confidential information shall be disclosed to authorized persons only.
- **Secret:** These are restricted information that represent a competitive advantage over competitors or a business secret. Access to information categorized as secret shall always be restricted to authorized individuals within the organization.

7.4.2.2. The Bank shall ensure the classification of all information always; this will ensure cost efficiency of all implemented controls.

7.4.2.3. The Bank shall determine the impact of a compromise on its information security triad while putting into consideration the classification level of each information.

7.4.2.4. The Bank shall implement security controls to protect its information, considering the classification level and impact of a compromise on the information to be protected.

7.4.2.5. The Bank shall assign an owner and a custodian to all information, either physical or digital.

7.4.2.6. The Information owner shall determine the appropriate classification for information within his/her control.

7.4.2.7. The information owner shall consult with the information custodian to determine appropriate controls for classified information.

7.4.2.8. The information custodian shall implement agreed controls for the protection of classified information.

7.4.2.9. The information owner shall manage classified information throughout the information life cycle; the information custodian shall ensure the security of classified information throughout the information lifecycle.

7.4.2.10. if the need for new categorization criteria arises, Information Security Steering Committee shall review the classification criteria and either approve or reject prior to implementation.

7.4.2.11. the information custodian shall ensure the backup of critical information; the custodian shall also keep a copy of the backup offsite.

7.4.2.12. The Bank shall label its memos, reports, and other outputs either in digital or physical form.

7.4.3. Classification and labelling requirements for all information assets

Type of Information	Labelling	Description
Public	No special requirement	• Information that may be released to the public, that does not benefit a competitor, negatively impact PremiumTrust Bank, or does not breach any confidentiality Information that may be published in any public forum without constraints either enforced by law or discretionary.
Internal Use	I Internal Use	• Information that is used internally but can be disclosed to authorized parties outside of the organization in a controlled manner. • This information must be disclosed to third parties only if a confidentiality agreement has been signed. • Disclosure is not expected to cause serious harm to PremiumTrust Bank, and access is provided freely to all employees through PremiumTrust Bank's intranet and email.

		Examples: Internal policies, standards and procedures, memos, organizational charts.
Confidential	Confidential	• Information distributed on a "Need to Know" basis that pertains in any way to customers, employees and financial programs or strategies developed by PremiumTrust Bank. • Information that is so sensitive that disclosure or usage would have a definite impact on PremiumTrust Bank business. • Information that may not be disclosed outside of PremiumTrust and represents a competitive advantage for the business • Further restrictions and controls need to be applied (e.g. very limited audience). • Cardholder data (PAN, name, expiry date), • Personally Identifiable Information - any information that can be used to distinguish or trace an individual's identity (Full names, drivers licence number, passport number, biometric data, taxpayer ID, personal address, personal telephone number, Bank Verification Number, photographic images etc.) Examples: corporate strategy document, business plans, preliminary reorganization memo, Merger and Acquisitions information etc.
Secret	Secret	Information or material, the unauthorized disclosure of could cause serious reputational damage to PremiumTrust Bank. Information or material whose disclosure can result in PremiumTrust Bank going out of business. Examples: Management meeting documentations, board papers and circulars.

		▪ Sensitive authentication data: this includes full magnetic stripe, CVC2/CVV2/CID, PIN/PIN block. Sensitive authentication data must never be stored and media containing sensitive data must not be handed over to any external entity or third party unless authorized by the management with proper business justification.

8. Cyber Security Policy

8.1. Introduction

This Cyber Security Policy is a formal set of rules by which those people who are given access to the Bank's information assets must abide. The main purpose of this policy section is to inform company users: employees, contractors, and other authorized users of their obligatory requirements for protecting the technology and information assets of the Bank.

8.2. Applicability

This policy is applicable to all staff and third parties accessing the Bank's information assets.

8.3. Scope

The Bank's computer hardware, system software, application software, network hardware and software constitute the scope of this policy.

8.4. Laws and Regulations

The Bank shall comply with the Nigerian Cyber Crime Law as stipulated in the Cyber Crimes (Prohibition, Prevention etc.,) Act 2015, Nigeria Data Protection regulation (NDPR) and other cyber regulations

The Bank shall comply with all cyber security requirements from financial regulatory bodies.

8.5. Email and Internet Acceptable Use Control

8.5.1. Objective

The objective of this sub-section is to ensure the secure use of the Bank's email and internet facilities.

8.5.2. Policy Statements

8.5.2.1. Users shall ensure the Bank's non-public information are transmitted on encrypted channels only.

8.5.2.2. Staff shall not install any software on the Bank's systems; only the IT support officers can execute such task for staff after obtaining appropriate approvals.

8.5.2.3. Staff shall use the Bank's provisioned mailboxes(firstname.surname@premiumtrustbank.com) for business communications only.

8.5.2.4. Staff shall not associate the Bank's provisioned mailboxes with their social media platform; the Bank prohibits opening of social media accounts using the Bank's provisioned email addresses.

8.5.2.5. Staff shall not receive or transmit critical business information using their personal mailboxes (abcdefgh@gmail.com).

8.5.2.6. The Bank prohibits staff from downloading software for use on the Bank's provisioned systems; the Bank's IT Support staff shall handle all software installations on the Bank's provisioned systems.

8.5.2.7. Staff shall ensure there are no lapses in implemented controls prior to accessing the internet; staff shall ensure the Bank's installed anti-malware solution is up to date prior to browsing the internet.

8.5.2.8. Staff shall enforce the necessary controls when dealing with classified information on and offline.

8.5.2.9. The Bank prohibits the use of its internet facilities for any form of illicit or unethical online activities such as pornography, fraud scheme, hoax, hacking, and related activities.

8.5.2.10. The Bank reserves the right to withdraw internet access from any user at any point in time; this may be due to business exigencies or in a situation where a user is compromising the Bank's network due to his/her internet activities.

8.5.2.11. Staff shall not disclose the content of emails received to unauthorized persons.

8.5.2.12. Staff shall securely delete a mail received in error and inform the sender provided, the sender is also a staff.

8.5.2.13. The Bank prohibits staff from engaging in activities that can negatively affect the Bank's network bandwidth such as video streaming, forwarding chain mails, large file downloads (games, movies, music files and other file types).

8.5.2.14. Due attention must be paid to security warnings that appear on our personal computers before clicking on unfamiliar links as they protect the Bank and customers from computer viruses and the like.

8.5.2.15. Staff shall not access, display, store, distribute, use, or create hacking tools and malware using the Bank's computing facilities and network.

8.6. Web Content Management

8.6.1. Objective

The objective of this sub-section is to provide guidance on content management on the entire Bank's web interface, which includes the website, the internet banking platforms and other internet-based customer facing platforms.

8.6.2. Policy Statements

8.6.2.1. Content Review and Approval

8.6.2.1.1. The sponsoring Management Executive, Group Head of the initiating business function and the Head Brand & Marketing shall approve proposed content.

8.6.2.1.2. The following conditions shall be satisfied before obtaining approval:

- Definition of the strategic objectives in creating the web page
- Outlining the specific web page content
- Detailing the proposed management of the web page
- Identifying potential graphics
- Detailing any third-party page links
- Establishing a budget
- Establishing a timeline for development

8.6.2.1.3. Approval will consider the following factors:

- Strategic relevance of the use of the Internet for communicating subject content.
- Consistency with the brand image, positioning, and personality of PremiumTrust Bank.
- Compliance with the PremiumTrust Bank Information Technology and Business standards.

- Consistency with other web pages to ensure integration and avoid duplication.
- All changes to the Bank's web interfaces shall adhere to the Bank's Change Management Policy.

8.6.2.2. Technical Requirements

- Use of interactive media is encouraged if used appropriately for the target audience.
- Files should be kept as small as possible to minimize download times.

8.6.2.3. Third-Party Service Providers

Only approved Third-Party Service Providers, adhering to the appropriate design and content requirements, shall develop and update web pages.

8.6.2.4. Managing a Web Page

Once a web page has been placed on the server, the content owner is responsible for:

- Maintaining a publishing schedule.
- Updating the content regularly (the minimum requirement is quarterly) and gaining approvals as described above.
- Responding to feedback/ questions.

8.6.2.5. Third-Party Pages

The Head, Brand and Marketing shall approve the addition of any third-party page links to the Bank's website.

8.6.2.6. Extranets

Extranets and closed intranets are valuable knowledge sources and can be established with selected third-party access. Deployment of Third-Party sites within the Bank's intranet

shall adhere to the approval procedures and standards detailed above.

8.6.2.7. The Bank shall establish a process for designating and controlling its web content versions.

8.6.2.8. The Bank shall take a periodic snapshot of it web contents.

8.6.2.9. The Bank shall develop a web content management strategy that will govern:

- Web Content Approval
- Web Content Publishing
- Web Content Modification
- Web Content Removal

8.6.2.10. The Bank shall test and ensure non-susceptibility of all web services (WSDL, SOAP and UDDI) in use on its domain to common vulnerabilities such as probing and coercive parsing.

8.6.2.11. The content approver and web content manager shall ensure publishing of content in line with the dictates of the Bank's Information Classification Policy.

8.6.2.12. The Bank shall ensure ease of use and availability of its web pages on a wide variety of browsers; the Bank shall ensure webpages are not browser dependent

8.7. Social Media Acceptable Use Control

8.7.1. Objective

The objective of this sub-section is to ensure effective management of the Bank's corporate image on social media platforms by preventing unauthorized

dissemination of confidential information and other activities that could negatively affect the PremiumTrust brand.

8.7.2. Policy Statements

8.7.2.1. Management Approval shall be obtained before the creation of social media accounts.

8.7.2.2. The Bank shall assign an administrator to all its social media accounts.

8.7.2.3. The administrators shall ensure strict adherence to the Bank's information security policies in the administration of the social media platforms.

8.7.2.4. The Bank shall setup an approval chain for its social media postings.

8.7.2.5. The approval chain and the platform administrators shall ensure non-disclosure of the Bank's confidential information on social media platforms.

8.7.2.6. Administrators shall take cognizance of copyright, privacy, fair use, financial disclosure, and other applicable laws while handling the Bank's social media accounts.

8.7.2.7. The administrators shall exhibit good professional conduct online by:

- Avoiding ethnic slurs, personal insult, display of racial or religious intolerance
- Avoiding misspelled words, bad grammar, and slangs
- Ensuring that conversations are positive and inclusive for customers and employees
- Refrain and totally avoid posting of customer and employee personal detail on social media platform

8.7.2.8. All employees of the Bank shall uphold high moral and ethical standards in

the use of their personal social media accounts, and interaction with the Bank's social media accounts. Employees shall ensure this by:

- Not posting on behalf of the Bank except expressly authorized to do so on social media platform
- Not including the Bank's logo or any of its trademark in a post unless authorized to do so
- Being open about their affiliations with PremiumTrust Bank, where and when required
- Being respectful of individual's right to express their opinion; whether critical or complimentary
- Refraining from work-related discussions on social media platforms
- Avoiding the use of jargons or slangs when interacting with the Bank's social media account
- Avoiding topics that depicts ethnic slurs, racial or religious intolerance
- Avoid sharing or associating with immoral posts such as pornography, post that depicts child abuse and are deemed obscene or offensive.
- Also prohibited are posts that are: defamatory, bring the Bank to disrepute, politically extreme, illegal, designed to defraud, designed to bully, threaten, harass, cause anxiety and inconvenience other.
- Exhibiting due care when sharing links on social media platforms
- Correct errors made in the process of interacting with or on the Bank's social media accounts

8.7.2.9. This policy applies to all multi-media, social network websites, blogs, and wikis for both professional and personal use of all staff and contractors while employed at PremiumTrust Bank.

8.7.2.10. If an employee (including contractors and affiliates) comments on any aspect of PremiumTrust Bank's business, they must clearly identify themselves as an employee and include a disclaimer. The disclaimer should be something like "the views expressed are mine alone and do not necessarily reflect the views of PremiumTrust Bank."

8.7.2.11. The Bank reserves the right to request that certain subjects are avoided, withdraw certain posts, and remove inappropriate comments from social (media) network sites, bearing the Bank's name and/or operations.

8.7.2.12. Employees (including contractors) should neither claim nor imply that they are speaking on PremiumTrust Bank's behalf unless explicitly mandated by the Bank's Branding & Marketing Group.

8.7.2.13. Employees or Third Parties shall not comment on the Bank's business or post information on behalf of the Bank during crisis unless explicitly authorized to do so. Where an unauthorized employee or Third-Party share information in any of the circumstances represented above, a disclaimer stating that the views expressed are that of the employee or Third-Party shall accompany such posts.

8.7.2.14. Staff must be careful about the type and amount of personal information provided on the Bank's social networking media sites.

8.8. Patch Management

8.8.1. Objective

The objective of this sub-section is to minimize the Bank's exposure to security threats

through effective management of its network, systems, application, and database vulnerabilities.

8.8.2. Policy Statements

8.8.2.1. The Bank shall task and equip Information Technology Team to handle patch testing and deployment, vulnerability mitigation and remediation, incident containment and eradication.

8.8.2.2. The Bank shall task its Information and Cyber Security Team with the vulnerability assessment of its infrastructure (Applications, Databases, Network and Systems).

8.8.2.3. The Information and Cyber Security Team shall perform all regulatory assessments and generate or obtain the corresponding clean reports; the ICS team shall carry out these assessments quarterly at the minimum.

8.8.2.4. The Information and Cyber Security Team shall draw up a schedule of non-regulatory scans targeted at improving the Bank's security posture; the team shall perform the scan based on their schedule and obtain applicable evidence of remediation from the Information Technology Team.

8.8.2.5. The Information and Cyber Security Team shall perform a vulnerability assessment of its applicable systems once there is a major change within the IT environment.

8.8.2.6. The Information and Cyber Security Team shall see to the annual performance of penetration test on the Bank's IT infrastructure; a Third-Party organization or competent internal resource shall handle the penetration test. The penetration test shall include:

- Network Layer

- Application Layer
- Database Layer
- Web Servers
- APIs
- People and Physical Layer

8.8.2.7. The Information and Cyber Security Team shall assess the Bank's wireless access points and ensure non-susceptibility to known wireless network vulnerabilities and exploitation techniques.

8.8.2.8. The Bank shall equip the Information and Cyber Security Team with tools capable of effectively monitoring and reporting on the Bank's IT infrastructure.

8.8.2.9. The Information and Cyber Security Team shall monitor the Bank's IT infrastructure and report when applicable on confirmed incidents and suspected Indicators of Compromises (IoCs).

8.8.2.10. The Information and Cyber Security Team shall categorize all identified vulnerabilities based on impact; the Bank shall adopt the vulnerability categorization below:

- **Critical:** These are vulnerabilities whose impact could adversely affect or bring to a halt, the Bank's business operations if exploited.
- **High:** These are vulnerabilities whose impact could disrupt the Bank's business operation if exploited.
- **Medium:** These are vulnerabilities whose impact is marginal on the Bank's business operation.

- **Low/Informational:** These vulnerabilities do not directly affect the Bank's business operation.

8.8.2.11. A risk assessment of identified vulnerabilities for which recommended fixes are not feasible shall be carried out; compensating controls shall be developed and documented.

8.8.2.12. Staff shall not make any temporary changes to information systems for the sole purpose of "passing" an assessment; the Staff's Disciplinary Committee shall handle identified cases of temporary system adjustment described above.

8.8.2.13. All patches shall be tested prior to deployment to production environment.

8.8.2.14. The Information and Cyber Security Team shall balance security with business objectives; the ICS team shall assess the impact of scans and schedule scans for period of minimal impact on the Bank's services and infrastructure.

8.8.2.15. Information Technology shall ensure no interference between the approved scanning tools and the target systems; scanning tools must be able to scan target systems without hindrances.

8.8.2.16. The Information Technology Team shall ensure the testing and deployment of critical security patches during the immediate maintenance window succeeding the patch release date.

8.8.2.17. The Internal Audit team shall independently audit the Bank's vulnerability management process; the audit shall focus on determining the effectiveness of the vulnerability management process in place within the Bank.

8.9. Teleworking Policy

8.9.1. Objective

The objective of this sub-section is to ensure that security of information and systems, accessed through teleworking are adequately protected.

8.9.2. Policy Statements

8.9.2.1. The statements below shall guide the implementation of Teleworking in the Bank**:** Two key features of Teleworking are:

- The worker is outside of the Bank's environment.
- Information and communication technologies are used to stay connected to the office. Possible scenarios for teleworking:
    - Staff are working from home or from a place that neither is their home or the organization (e.g., coffee shops, hotels, planes, etc.).
    - Staff are using fixed or mobile devices (e.g., PCs, notebooks, tablets, smartphones, etc.).
    - Staff are using public or private communication networks (e.g., Internet and Extranet).

It Is important to note that, although all devices are at risk of being lost or stolen, the nature of mobile devices (e.g., size, portability, and value) increases this risk.

To protect the Bank's information assets and supporting infrastructure, teleworking shall be implemented in line with the following requirements:

- Access to the Bank's core banking solution shall be excluded from resources available for teleworking.
- Adequate controls shall be implemented based the Bank's Information Classification to ensure only approved resources and services are

available for teleworkers.

- Information classified as confidential, or secret shall be unavailable to the teleworker.
- Access controls shall be in place for teleworkers. These shall include but shall not be limited to the following: passwords, two-factor authentication, use of VPN on communication channels).
- Members of staff shall continually be notified of their roles and responsibilities in securing the Bank's resources while teleworking and making clear that information compromise related to a lack of caution could result in disciplinary proceedings and even legal action.
    - Only when unavoidable should staff take, send, or print hardcopies of confidential documents out of secure Bank locations.
    - Printing of documents should be restricted except where unavoidable.
    - If necessary, to handle confidential hardcopy documents, they should be kept in locked cabinets when not attended to (clear desk policy).
    - Destruction of documents should be by shredding.
    - Documents being transported should be recorded and locked away from unauthorized access.
    - Asset owners and those responsible for managing provision of teleworking equipment must ensure, on termination of the arrangement, the secure return or disposal of all equipment and/or information, in electronic or paper form, held by the teleworker.

8.9.3. Reference(s)

i. Asset Management Policy

ii. Identity and Access Management Policy

iii. Network Management Policy

iv. Information Management Policy

v. System Compliance Policy

vi. Incident management Policy

vii. Change and Release Policy

9. Supply Management Policy

9.1. Introduction

This policy defines the standards for governance of procurement process in the Bank. It serves as a guide to security standards for all business functions to follow while managing suppliers and purchases on behalf of the Bank.

9.2. Applicability

This policy is applicable to all members of staff involved in purchases and supplier management. The policy applies to suppliers as well.

9.3. Scope

Service acquisition, management, and supplier management

9.4. Vendor Selection Process Control

9.4.1. Objective

The objective of this policy is to ensure that vendors to be selected for identified services meet specific security standards and possess the capacity to execute the outsourced

service.

9.4.2. Policy Statements

9.4.2.1. The contractor selection process shall include the Bank's security requirements; this formal process shall ensure that all security requirements are met. In addition, the conditions for service and the required security controls shall be formally specified and agreed to by the contractor.

9.4.2.2. The Bank shall establish relevant information security requirements for its vendor selection process.

9.4.2.3. The vendor shall demonstrate adequate knowledge and competence required to continuously provide and support the required service.

9.4.2.4. The Bank shall ensure that prospective vendors have the capabilities to securely process its information.

9.4.2.5. The Bank shall ensure that prospective vendors adhere to the requirements of the standards that govern the service to be outsourced.

9.4.2.6. Where applicable, the service provider shall have relevant certification(s) in the field of practice.

9.4.2.7. The outsourcing party shall demonstrate ability to ensure the required level of service availability is maintained.

9.5. Outsourcing Management

9.5.1. Objective

It is often necessary that the responsibility for information systems processing, development and/or maintenance be designated to external companies or individuals. In these circumstances, it becomes vital that the security (i.e. confidentiality, integrity, and availability) of the Bank's information is maintained. To facilitate this. Contracts

between the Bank and contractor(s) shall be established. These contracts shall stipulate the security requirements and practices to be fulfilled.

The purpose of this policy is to establish management accountability and the minimum-security requirements for outsourcing. This policy will ensure the implementation of appropriate measures to minimize the risk of:

- Information integrity and confidentiality compromise
- Computer performance disruption or degradation
- Incurring reputational damage; and/or
- Poor or late delivery of service by outsourced contractor(s).

9.5.2. Policy Statements

9.5.2.1. A formal risk assessment shall be performed prior to considering the utilization of outsourced services; every outsourcing contract negotiation requires a risk assessment to be performed. Depending on the risks associated with the Bank's data that will be accessible by external parties and the Bank's processes that will be controlled by external parties, relevant areas of IT security shall also be analyzed for security risks.

Risk assessments will enable the Bank to identify the risks associated with the function being outsourced, as well as the risks associated with the outsourcing company of choice. This will enable the Bank to choose an outsourced contractor whose security practices meet the minimum- security requirements of the Bank.

The Bank shall:

- Subject the selection of contractors and the delegation of authority to a formal process.

- Identify risks and assess security practices employed by contractors.
- Agree on security controls, approve transfer, and establish formal agreements prior to outsourcing responsibility for systems development.
- Identify sensitive or critical systems that are better retained in-house.

9.5.2.2. The Bank shall ensure that outsourced service providers comply with all applicable PremiumTrust security policies and procedures; these include (but are not limited to) effective incident management, access control and change control procedures based on the Bank's policies. Outsourced service providers shall also maintain the integrity and confidentiality of all information obtained during their work in the Bank.

9.5.2.3. Where applicable, selected vendors shall sign Non-Disclosure Agreements with the Bank prior to the execution of contracts.

9.5.2.4. At the expiration of all outsourced contracts, the Bank shall withdraw access to its information resources.

9.5.2.5. Where applicable, the Bank shall sign escrow agreements with selected vendors.

9.5.2.6. The Bank shall regularly monitor, review, and audit supplier service delivery.

9.5.2.7. Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.

9.5.2.8. Changes to existing contracts with suppliers shall be documented and duly signed off by representatives of the Bank and the service provider.

9.5.2.9. A re-assessment of risks shall be conducted by the Information & Cyber Security Group for changes to the provision of services by suppliers,

considering the criticality of business information, systems, and processes involved.

9.5.2.10. The Information & Cyber Security Group shall monitor the activity of outsourced system development.

9.5.2.11. Prior to sign-off, the Information & Cyber Security Group shall ensure that the contract terms agreed between the Bank and suppliers complies with the Bank's information security policies.

9.5.2.12. All security requirements shall be addressed in a contract agreed between the parties; a suitable contract, which meets the Bank's requirements, shall be entered. These requirements should address the security risks, controls, and procedures for information resources in the contract between the parties.

9.5.2.13. The contract should address as a minimum:

- How the legal requirements are to be met.
- What arrangements will be in place to ensure that all parties involved in the outsourcing, including subcontractors, are aware of their security responsibilities.
- How the integrity and confidentiality of the Bank's information resources are to be maintained and tested.
- What physical and logical controls will be employed to restrict and limit access to the Bank's critical information resources.
- How the availability of services is to be maintained in the event of a disaster.
- Compliance to PremiumTrust Information Security Policies.

- Target and unacceptable levels of service.
- Intellectual property rights, copyright assignment and protection of any collaborative work.
- Procedures to maintain a list of rights and privileges of users authorized to use the available services.
- The right to audit contractual responsibilities or have those audits performed by a third party.
- The establishment of an escalation process for problem resolution.
- Contingency arrangements.
- A defined Change Management Process.
- Controls to ensure protection from malicious software.
- In the case of outsourced software development:
    - Licensing arrangements and source code ownership.
    - Certification of the quality and accuracy of the work performed.
    - Escrow arrangements.
    - Contractual arrangements for the quality of the code; and
    - Testing before installation to detect malicious code.

Where the Bank's security requirements cannot be enforced, the reason and associated risks must be identified and signed off by the Chief Information Security Officer (CISO).

9.5.2.14. Responsibility for managing the relationship with the outsourced service provider shall be assigned to a designated individual with sufficient technical skills and knowledge.

9.5.3. Reference(s)

i. Identity and Access Management Policy

ii. Application Management Policy

iii. Information Management Policy

iv. Incident Management Policy

v. Change Management Policy

10. Incident Management Policy

10.1. Introduction

Incidents are disruptions to normal operations of an entity. Security incidents do not necessarily disrupt the normal operations of an organization but compromises one of the three elements (Confidentiality, Integrity, and Availability) of information and information processing facilities.

The Bank formulated this section of the policy to ensure effective maintenance of the Confidentiality, Integrity, and Availability of information resources within the Bank through timely identification and handling of incidents.

10.2. Applicability

This policy is applicable to all members of staff (permanent and temporary), service providers and all system resource utilized by the Bank for the execution of its business processes.

10.3. Scope

All system resources and services managed by both the Bank and Third Parties.

10.4. Incident Logging and Tracking

10.4.1. Objective

The objective of this sub-section is to ensure that identified incidents are efficiently logged and tracked.

10.4.2. Policy Statements

10.4.2.1. All types of incidents shall be defined and categorized in terms of their severity; all incidents shall be defined according to the following categorizations based on the impact of the incident:

- Business Critical - 5
- High - 4
- Moderate - 3
- Low - 2
- Minimal - 1

This definition and categorization of incidents shall assist in assessing the associated risk to the business and the urgency with which the incident shall be responded to. This shall be performed on a Bank-wide basis.

10.4.2.2. All incidents with a severity of 2 or higher shall be recorded; Evidence (for incidents with severity 2 or higher) shall be gathered within the stipulated response time to ensure that the incident is adequately addressed.

10.4.2.3. Users and contractors shall be made aware of what constitutes an incident and how to react to incidents; Users of information resources shall be made aware of the different types of incidents and the associated Incident Management Procedures. They shall be required to note and report any observed or suspected security weaknesses in or threats to systems or resources. Incidents shall be reported to IT Service Desk or Information & Cyber Security Group.

10.4.2.4. Users and contractors shall not attempt to test or identify any suspected weakness, as testing/analysing weaknesses shall be interpreted as a potential misuse of the system.

10.4.2.5. The Bank shall establish a formal incident response plan. The plan shall be backed up by an incident management procedure that shall document what actions to be taken in the event of a potential or actual incident. The procedures shall cover all potential types of security incident including system failures, errors resulting from incomplete or inaccurate data and confidentiality breaches. The procedures shall also include activities to perform for the effective gathering of evidence close to the time of the incident either for problem analysis and/or litigation. The procedures shall cover identifying the cause of an incident, implementing remedies to prevent recurrence, and communicating with users and others involved in a recovery situation.

10.5. Incident Resolution Management

10.5.1. Objective

The objective of this sub-section is to ensure that incidents are efficiently resolved within stipulated timelines.

10.5.2. Policy Statements

10.5.2.1. Security administrators shall have documented procedures to monitor and report all significant security events in line with the Incident Management Policy.

10.5.2.2. Recorded incidents shall be responded to in accordance with the Incident Management Procedure; Actions taken to recover from security breaches and to correct system failures shall be carefully and formally controlled in

accordance with the Incidence Management Procedure. Suitable feedback processes shall be implemented to ensure that the people reporting the incidents are notified of results after the incident has been dealt with and closed. These incidents can be used in user awareness training.

10.5.2.3. Staff with responsibilities for security breach response are periodically trained.

10.5.2.4. Incident Management Procedures shall ensure that all security control violations are investigated promptly and that escalation procedures are invoked wherever necessary.

10.6. Root Cause Analysis

10.6.1. Objective

The objective of this sub-section is to ensure that the source or origin of identified incidents are determined in other to prevent a reoccurrence of known incidents.

10.6.2. Policy Statements

10.6.2.1. Reported incidents shall be analyzed for trends; Incident logs shall be reviewed to detect any trends, which may identify risks to the Bank. The analysis shall include:

- Identifying the cause of the incident
- Assessing the impact of the incident; and
- Developing solutions to prevent the reoccurrence of the incident

10.6.2.2. The methodology that was used to detect and resolve the incident shall be documented on the knowledgebase of the Incident Management Portal. This shall include the tools used for the forensic investigation.

10.6.2.3. The lessons learnt shall be documented and used to improve the Bank's security posture.

10.6.2.4. The Bank shall define and apply procedures for the identification, collection, acquisition, and preservation of information, which can serve as evidence.

10.7. Attack Curtailment and Counter Response

10.7.1. Objective

The objective of this sub-section is to ensure that identified incidents are controlled, restricted to affected environment or host and effective controls are put in place to avoid a reoccurrence of the incidents.

10.7.2. Policy Statements

10.7.2.1. Unresolved incidents shall be reviewed and actioned; all unresolved security incidents shall be reviewed to ascertain what remedial action has been taken.

10.7.2.2. Critical incidents affecting the Bank shall receive immediate attention. If required, the necessary actions shall be taken to isolate the affected areas; the isolation of affected areas is critical to the Bank's business. This shall minimize the risk of unaffected areas being affected by the critical incident and decrease the overall impact on the Bank's information resources.

10.8. Cyber Threat Intelligence (CTI)

10.8.1. Objective

The Cyber Threat Intelligence (CTI) policy defines guidelines for obtaining cyber threat intelligence that will help ensure proactive awareness of, and response to cyber threats.

Knowing the methods and tools attackers are most likely to use can help PremiumTrust Bank better prepare to thwart incoming attacks.

10.8.2. Policy Statements

10.8.2.1. PremiumTrust Bank shall implement a CTI program to ensure PremiumTrust is

aware of and able to respond to emerging threats, attack vectors and indicators of attacks/compromise to its information assets.

10.8.2.2. Information and Cyber Security Group shall be responsible for PremiumTrust Bank's CTI program.

10.8.2.3. The Bank shall subscribe to external threat intelligence providers, intelligence sharing groups, and relevant agencies to keep abreast of emerging cyber threats and vulnerabilities.

10.8.2.4. The Information and Cyber Security Group shall review internal intelligent data sources continuously for prompt cyber threat identification and remediation. The internal intelligent data sources include security events generated by IT Infrastructure, e.g., systems and security logs, database activity logs, malware detection logs, network traffic analysis, etc.

10.9. Reference(s)

i. Network Management Policy

ii. Supply Management Policy

iii. Business Continuity Management Policy

11. Business Continuity Management Policy

11.1. Introduction

The prolonged unavailability of normal business services has dire consequences on the financial and reputational standing of the Bank. It is therefore necessary to minimize interruptions to business activities.

The Bank developed its **Business Continuity Management Policy** to establish the requirements for maintaining effective and continuous business operations in the event of failures and disasters.

11.2. Applicability

This policy is applicable to all members of staff (permanent or temporary), service providers and all critical system resources utilized by the Bank for the execution of its business processes.

11.3. Scope

All human resources, critical system resources, services, and physical assets in use within the Bank.

11.4. Business Continuity Planning

11.4.1. Objective

The objective of this policy is to ensure that Business Continuity Management plans and procedures are in place to facilitate the normal functioning of the Bank's critical business activities in the event of failures or disasters.

11.4.2. Policy Statements

11.4.2.1. A strategy for Business Continuity Management shall exist duly approved.

- The strategy for Business Continuity Management shall serve as a single framework on which business continuity plans and procedures shall be developed throughout the Bank.
- Business Unit strategies shall identify the business activities for which there is a necessity and priority for recovery, based on criticality.
- When determining the criticality of applications and the systems and infrastructures that support them, consideration needs to be given to the impact that the loss or unavailability of these will have, particularly in terms of the following:
    - Loss of business activities and services to customers (loss of employee

and customer good will);

- Financial impact as determined by the loss of revenue.
- Legal impacts in terms of legal, contractual, governmental, and regulatory requirements.
- Impact on the corporate image and reputation of the Bank
- Interaction with other processes, services, and applications
- Interaction with third parties

- The overall approach to be followed when developing the corresponding Business Continuity Management plans and procedures can then be established; and
- All system recovery and response timeframes shall be quantified.

11.4.2.2. Information Technology Steering Committee shall make decisions on the level and scope of Business Continuity Planning after fully considering business risks, impacts and legal responsibilities as well as the costs of various continuity planning options, which the Bank may pursue.

11.4.2.3. Prior to developing Business Continuity Management plans and procedures, formal risk and impact analysis shall be performed to identify business critical processes and systems; risk analysis should consider the probability of a disaster or failure occurring and the potential impact of such an event. The events should then be prioritized and addressed accordingly.

11.4.2.4. Business Continuity Management plans and procedures shall be developed to align with the agreed upon strategies; these plans and procedures shall be formally documented, communicated, and practiced throughout the Bank and shall cover all information resources. The plans and procedures

should initiate the recovery of information resources in the event of a disaster or system failure. These plans and procedures aim to deliver the uninterrupted (or minimally interrupted) availability of all critical information resources.

They shall contain procedures to keep critical business activities and services running and shall not merely contain fallback arrangements for computer services. The plans and procedures shall consider, amongst others, the following:

- Identification and prioritization of critical business processes
- Potential impact of various types of disasters
- Identification and agreement on the key resources and responsibilities
- Emergency arrangements for accommodation and communication
- Conditions, responsibilities, and authority for invoking emergency procedures.
- Responsibilities for staff awareness in the emergency procedures
- Training of responsible persons
- Testing strategies and schedules
- Maintenance schedules
- Relationships with other business continuity plans and procedures
- Fall-back arrangements for computer services
- Backup strategies and locations
- Suppliers and support contacts
- Inventory lists for hardware, software, documents, and data

- Steps for recovery of processes and systems
- Restoration back to permanent facilities
- Legal requirements
- Security arrangements
- Review of the plans
- Change management procedures; and
- Analysis of consequences/causes of disaster.
- These plans and procedures shall be developed in conjunction with Group Heads or appointed designates.
- When developing plans, the solutions implemented should be aligned to the risk associated with the area addressed.

11.4.2.5. The Business Continuity Management Plan shall incorporate a Disaster Recovery Plan for the recovery of IT services.

11.4.2.6. All information used in the decision-making process for continuity planning shall be formally documented (e.g., risk analysis results, insurance costs, etc.).

11.4.2.7. Business Continuity Management plans and procedures shall include the responsibilities for carrying out effective recovery, the emergency procedures to be followed and the conditions under which these procedures shall be activated.

11.4.2.8. Business Continuity Management plans and procedures shall contain sufficient details to permit timely resumption of business activities; the level of details shall be sufficient for the plans and procedures to be executed by the individuals responsible for recovery.

11.4.2.9. To ensure continuity and recovery of processes and services that have been outsourced to another organization, the following shall be taken into consideration:

- Continuity and recovery requirements shall be included in contracts with organizations providing business process and facilities management.
- Contracts shall address disaster notification, requirements, and procedures; communication channels and methods; public relations co-ordination; effects on service levels; testing liaison and frequency; independent auditing of recovery and continuity plans.
- Annual reviews shall be conducted to ensure continuity and recovery plans for the Bank and the service provider work effectively with each other.

11.4.2.10. Relevant users shall be made aware of their responsibilities with regards to the Business Continuity Management plans; users shall be educated on business continuity procedures and the emergency processes to be followed in the event of a disaster. Individuals responsible for implementing recovery shall be made aware of their responsibilities.

11.4.2.11. Business Continuity Management plans and procedures shall include redundancy arrangements for business processing sites, systems, and equipment, if these become unavailable; Disaster at the main sites of business activities could necessitate moving business activities to a temporary site. These redundant sites should be available when needed and effective recovery shall be possible at these sites.

11.4.2.12. The security of disaster recovery facilities and systems shall be at the same level as security practices on the main site of business activities.

11.4.2.13. Business Continuity Management plans and procedures shall be tested. The frequency shall be in accordance with pre-defined schedules; the testing of continuity management plans and procedures shall be practised to verify that the plans and procedures are relevant and can still facilitate recovery within required timescales. Individual components of the business continuity management plan shall be tested frequently. Testing of the plans and procedures shall occur when there are major changes to the business operations that govern these activities. All tests, and the results thereof, must be recorded.

11.4.2.14. Reviews and updating of Business Continuity Management plans and procedures shall be carried out in accordance with a review schedule; the review schedule shall provide for the review of business continuity management strategies, plans and procedures once a year. In addition, compulsory reviews shall be performed when there are major changes to business activities. Maintenance practices shall ensure that all business continuity plans and procedures are consistent with the agreed upon strategy. These reviews will assist in identifying new requirements for business continuity management and facilitate the subsequent amendments to the plans and procedures.

Any necessary updates to the Service Level Agreement shall be considered.

11.4.2.15. Updates to the Business Continuity Management plans shall comply with the Bank's Change Management Control Policy.

11.4.2.16. The Bank's critical information assets shall be covered by appropriate insurance, the loss or unavailability of which, could have significant financial impact.

11.4.2.17. Business Continuity Management plans and procedures shall have distinct

ownership; the designated owner of Business Continuity Management plans and procedures shall ensure that these plans and procedures are updated and tested as required and are consistent with the overall strategy of business continuity.

11.4.2.18. Critical Application and system inventories identified will be maintained and reviewed annually.

11.4.2.19. Technical infrastructures (e.g., LANs) and their services (e.g., e-mail) and the impacts of their loss on the business shall be considered.

11.4.2.20. Impacts of loss of Electronic Data Interface (EDI) transactions, SWIFT transactions and other transactions involving third parties shall be considered when determining criticality.

11.4.2.21. Plans shall be developed to level which allows recovery of business functions without including spurious details which may cloud key issues or create a necessity for frequent updating.

11.4.2.22. A Business Continuity Management team shall be established to co-ordinate business continuity issues in the event of an emergency.

11.4.2.23. The Bank's Incident Management Plan shall be fully integrated into the Business Continuity Management Plan.

11.4.2.24. Business Continuity Management plans and procedures shall be readily available but restricted to authorized individuals.

11.4.2.25. Copies of Business Continuity Management plans and procedures shall be held off-site in a secure location:

- Copies of Business Continuity Management plans shall be stored separately from the originals to prevent simultaneous destruction with the

originals.

- A remote location, at a sufficient distance to escape damage from disaster at the main site, shall be chosen. This will facilitate effective recovery in the case of a disaster at the main site of business activities.
- An off-site location should offer access out of normal business hours.

11.4.2.26. Copies of critical manuals, records, files, etc. needed for continuity planning should be held in a secure off-site location.

11.4.2.27. Business Continuity Management Plan shall take into cognisance Capacity planning; this shall be in accordance with the Bank's Capacity Planning Policy.

11.5. Disaster Recovery Management (Information Technology)

11.5.1. Objective

The objective of this sub-section is to ensure effective recovery of IT services in the event of a major incident or an IT disaster.

11.5.2. Policy Statements

11.5.2.1. Information Technology Group shall develop and regularly update the Disaster Recovery Management Plan and Procedures.

11.5.2.2. Information Technology Group shall maintain separate documentations for recovery of all IT services supported by the Group.

11.5.2.3. For critical services (e.g., core banking services), Information Technology Group shall maintain a high availability architecture for the service delivery.

11.5.2.4. Information Technology Group shall maintain a service catalogue detailing the criticality of services, which shall be used to prioritize IT Disaster Recovery activities.

11.5.2.5. Information Technology Group shall test the IT Disaster Recovery Plan regularly based on agreed schedule.

11.5.2.6. Outcomes from the test shall be used to update the IT Disaster Recovery Plan.

11.5.2.7. Information Technology Group shall maintain an up-to-date backup of critical data, and this shall be carried out in accordance with the Bank's Backup Policy.

11.5.2.8. Information Technology Group shall ensure that the IT Disaster Recovery Plan take cognizance of the Bank's Information Security Policy.

11.6. Data Backup/Restore & Archive Management

11.6.1. Objective

The objective of this sub-section is to ensure the Bank effectively manage its data redundancy process.

11.6.2. Policy Statements

11.6.2.1. Each Business Group shall make available to Information Technology Group the following information to ensure effective backup of their data:

- Identification of critical data, information and software that need to be backed up.
- The retention periods for backups of critical business information and archived copies.
- The frequency and type of information backup based on the business process requirements.

11.6.2.2. Information Technology Group shall develop a Backup Strategy to effectively provide redundancies for critical business data.

11.6.2.3. Actions to be taken in case of temporary or permanent loss, destruction or unavailability of information shall be clearly documented, forming a part of the Bank's standards and procedures.

11.6.2.4. Critical data, information and software shall be backed-up, according to the backup strategy.

11.6.2.5. Backups and backup procedures shall be tested regularly. The frequency shall be in accordance with pre- defined schedules; testing procedures shall be in place to verify that backups meet business continuity requirements and that they are, accessible and reliable when needed.

11.6.2.6. Appropriate storage media shall be made available for both data backup and restoration

11.6.2.7. Backup information and facilities shall be readily available to implement disaster recovery and restricted to authorized individuals.

11.6.2.8. Critical backups and recovery procedures shall be held off-site in a secure location. To prevent simultaneous destruction of backup and original copies, backups shall be stored offsite in a secure location.

11.6.2.9. All application data, which is required for recovery, shall be kept in a secure off-site facility; a copy of the most current critical software, application programs, documentation, and other contingency/disaster records shall also be kept off site.

11.6.2.10. Copies of documentation pertaining to backups shall be stored with the backup.

11.6.2.11. Backup information shall be given an appropriate level of physical and environmental protection in accordance with the Physical and Environmental policy; the level of protection accorded to off-site copies of

backup information shall be the same as that of on-site backup to ensure consistency.

11.6.2.12. A backup register shall be in place, maintained and reviewed on a regular basis; the backup register shall identify all information and systems to be backed-up. It shall also include the nature, timing, and extent of backups. The register should be reviewed for completeness on a regular basis and updated whenever new systems are introduced.

11.6.2.13. Copies of all contingency and recovery plans should be held in printed form off site in a secure location

11.6.2.14. All backups and the testing thereof shall be logged. The logs shall be reviewed on a regular basis.

11.6.2.15. End users shall be responsible for ensuring that data under their direct control are backed-up; this shall apply to data stored on user's PCs/laptops. Users shall ensure that data they are responsible for are backed-up adequately and stored securely.

11.6.2.16. Authorized staff of Information Technology and Compliance, only, shall be responsible for the retrieval of backup media from offsite locations.

11.6.2.17. The authorized staff shall obtain approval from the Chief Information Officer prior to the retrieval of backup media from offsite locations.

11.6.2.18. The authorized staff shall return retrieved media to the offsite location not later than after 48hours of fulfilling the purpose for which it was retrieved.

11.6.2.19. The authorized staff shall sign the logbook at the offsite location during retrieval and at the return of backup media.

11.7. Capacity Planning and Management

11.7.1. Objective

The objective of this sub-section is to ensure the Bank has adequate resources in terms of infrastructure, software, skilled personnel to sustain all services to customers and to ensure all business processes function adequately without capacity challenges.

11.7.2. Policy Statements

11.7.2.1. Current and projected capacity levels of the Bank's critical information resources shall be identified, monitored, and planned for, to ensure the availability of adequate capacity levels.

11.7.2.2. Strategies shall be established for the planning of capacity at all levels.

11.7.2.3. Capacity plans shall be reviewed and updated regularly, on a basis determined by the CIO. The frequency of the review shall consider changes to business and system requirements and changing capacity levels.

11.7.2.4. All critical resources shall be identified and planned for. Consideration shall be given to the classification of the information resource and the information stored/processed on the information resource, in accordance with the Physical and Environmental Policy.

11.7.2.5. The minimum required performance levels for all critical assets shall be identified and incorporated into the capacity plan.

11.7.2.6. Maximum threshold capacity levels (i.e., the highest acceptable capacity level) for critical assets shall be documented to allow effective and timely capacity planning.

11.7.2.7. Projected critical information resource performance and capacity levels shall be identified and planned for; current and projected performance

and capacity demands shall be recorded to ensure that adequate processing power and storage are available. Projections shall take into consideration new business, changes to existing systems, system requirements, current and projected trends in information processing and lead times to procure such resources.

11.7.2.8. Critical information resource performance and capacity levels shall be monitored on a continuous basis. Performance shall be constantly monitored to provide timely and accurate information.

11.7.2.9. Changes to capacity plans shall be reflected in Business Continuity Management Plans; Capacity changes, because of increasing network usage or changes in the network architecture, shall be reflected in Business Continuity Management Plans to ensure the continued recovery of systems and processes.

11.7.3. Reference(s)

i. Identity Management Policy

ii. Network Management Policy

iii. Change Management Policy

iv. Incident Management Policy

12. Physical and Environmental Control Policy

12.1. Introduction

Information processing facilities must be secured from unauthorized access, damage, or interference. Physical security measures must be in place to ensure the security and integrity of information processing facilities and the information assets located within.

Environmental security conditions must be implemented to reduce exposure to environmental threats.

12.2. Physical Security

12.2.1. Policy Statements

12.2.1.1. Securing the Office Premises

- PremiumTrust premises must have a well-defined and secure perimeter.
- The main entry of PremiumTrust premises must be secured using a manned reception and appropriate controls to secondary entrances.
- Access of all employees must be restricted to their relevant work areas.
- All doors and windows shall be locked, when unattended, beyond working hours.
- Directories and internal books identifying locations of organizational information processing facilities, or any other sensitive or secure area shall not be readily available or accessible to the public.
- Knowledge or access of the "secure areas" [e.g., server room, etc] shall be given to personnel or third party on a need-to-know basis.
- All incoming equipment must be declared at the security gate and a gate-pass must be issued for the same. Any outgoing equipment must be accompanied by a gate-pass approved by a designated official.

12.2.1.2. Security of Office Equipment

- The site chosen to locate information processing equipment must be secured from theft, physical intrusion, and environmental hazards.
- Support functions and equipment e.g. photocopiers, shall be sited

appropriately within the secure area to avoid demands for access, which could compromise information.

- Movement of any office equipment needs to be authorized by the Group Head of the department.
- Movement of all equipment within and outside premises must be accompanied by a gate-pass authorised by the business owner of the equipment.

12.2.1.3. Securing Access to Sensitive Areas

- All information processing facility must have a well-defined perimeter and additional controls shall be in place to secure critical or sensitive information.
- Access to secure areas must be strictly restricted. e.g., access to server rooms may be controlled and restricted to authorized personnel like System administrators who need to perform their duties.
- Use of authentication mechanisms (e.g., access card) must be considered for access to secure areas.
- In secure areas, rooms must be equipped with doors, which are resistant to forcible entry.
- Signs indicating "Authorized Personnel Only" or a similar message will be prominently posted at all entrances any secure area.
- Knowledge or access of the "secure areas" [example: server rooms, equipment room, etc] shall be given to personnel or third party on a "need-to-know" basis.
- Server rooms, backup storage rooms and power supply rooms will not be

visible or identifiable from the outside; that is, no windows or directional signs will exist.

- "Secure areas" shall be locked when vacant.

12.2.1.4. Securing Premises from Third Party and Visitors

- Public access, delivery and loading areas shall be controlled and, if possible, isolated from information processing facilities.
- The date and time of entry and departure of visitors and third parties and the purpose of visit must be recorded in a visitor's log.
- The date and time of entry and departure and the purpose of entry of authorized personnel (including employees of outsourcing agencies) outside normal business hours or assigned hours of work must be recorded in a log.
- All visitors must be requested to wait at the reception and the employee being visited will accompany the visitor with him inside the office premises.
- No employee is authorized to take any visitor near user workstations. He shall keep his entry restricted to the discussion rooms.
- Visitors and third parties will be allowed entry to server room for authorized and specific purposes only. They must not be permitted unsupervised access to computer and communication rooms.

12.2.1.5. Securing Information Storage Media

- All information storage media (e.g., hard disks, USB, CD-ROMs, etc) containing sensitive or confidential data will be physically secured, when not in use.

- No information storage media must be taken outside the server room or storage area, unless authorized by management.
- Physical access to magnetic tape, disk and documentation libraries will be restricted to authorized personnel based on job responsibilities.
- Back-up media will be stored in fire resistant safes or cabinets. A copy of all backup media shall be maintained at an offsite location. The identified offsite location, for storage of backup media, shall have prior approval from Management.
- Visitors and third parties will not be allowed to bring along their laptops, or any other external storage devices, unless authorized by PremiumTrust officers.

12.2.1.6. Securing Offsite Facilities

- Adequate redundancy must be provided to the existing hardware and other sub systems so that there is business continuity in the event of a disaster; by way of duplication / replication of the already existing systems at another cost-effective location.
- Reliable Vendors must be identified to procure critical equipment and other office material at any given point in time in the event of a disaster.
- Fall back equipment and back-up media must be stored at a safe distance to avoid damage from disaster at the main site.
- The physical and environmental safeguards available at the off-site location must provide the same level of security, at a minimum, as at the primary site.

12.2.1.7. Cabling Security

- Power and telecommunication lines used for information processing facilities must be underground, where possible, or subject to adequate alternative protection.
- Network cabling will be protected from unauthorized interception or damage due to environmental hazards e.g., by using conduit or by avoiding routes through public areas.
- Power cables will be separated from communication cables to prevent interference.

12.2.1.8. Physical Security of Laptops

- Laptops must not be left on the desk or in the work area or any other visible location overnight.
- Laptops must not be left unattended in cars or public places like an airport.
- Laptops must never be checked in as luggage, while travelling. It must always be hand carried in a briefcase or a laptop carrying case.
- When staying in hotels, users must lock their laptops in cupboards when they are not present. If room security is not of a high order, then users must take it with them.
- A record of laptop's make, model, and serial number should be kept.
- In the event of a laptop being stolen, the concerned employee must file a police report immediately. He must also notify the IT and ICS departments about the theft, within three business day.
- Any removable media devices, such as CD Writers, Zip drive and Tape drives, will not be added to individual laptops unless authorized by the

Head IT and CISO.

- Modems will not be added to individual personal computers unless authorized by the Head IT and CISO.

12.2.1.9. Clear Desk and Clear Screen

- Computer terminals and printers will not be left logged on, when unattended. Key locks, power-on and screensaver passwords, or other controls will be used to protect them when not in use.
- Computer media, like CDs, tapes etc. containing confidential information will not be left unattended. They will be stored in suitable locked cabinets when not in use, especially after working hours.
- Files and other papers (non-electronic format) that contain sensitive or confidential information will be protected from unauthorized access. Users will not leave such papers unattended on printer trays, photocopiers, fax machines or their desks.
- 'Confidential' information and storage media will be locked (ideally in a fire-resistant safe or cabinet), when not required.

12.2.1.10. Equipment Security

- The placing of any equipment shall be decided based on the criticality of the equipment and the information carried in the equipment.
- The placing shall be such that unnecessary access into work areas is restricted.
- Eating, drinking, and smoking shall be controlled in the office premises to minimize the risk of physical threats like fire, smoke, water etc.
- Combustible materials shall not be stored in office premises.

- All equipment must be maintained, in accordance with manufacturer's specifications.
- Only authorized maintenance personnel must be allowed to service or perform repairs on equipment. A log must be maintained of all repairs or service work.
- If equipment must be sent offsite for repairs, the confidentiality and integrity of any information shall be ensured. The entire data available on the equipment shall be backed up on a device and entirely removed from the equipment.
- PremiumTrust Management shall authorize any equipment used to process the organization's information. The security standards documented within the security policy will apply to all equipment and information regardless of location.
- Any equipment or media taken outside the organization's premises must be controlled, secured, protected, and insured.
- For cases of remote access to information or working from home, risk assessment shall be performed, and controls shall be applied based on the risk levels.
- Employees or contractors shall not remove property off premises, without prior authorization. Equipment, information and software shall be logged out when taken offsite and logged back in when returned.
- In the case of equipment left unattended or not in use, the custodians of these equipment must be notified and follow protocol by logging the same and storing away the materials till a use has been assigned to the equipment.

12.3. Environmental Security

12.3.1. Policy Statements

12.3.1.1. Ensuring Suitable Environmental Conditions

- The air-conditioning and humidity levels must be monitored in the server room.
- Smoking is strictly prohibited inside the office area and may be permitted in the adjoining open area.
- Eating and drinking inside server room is strictly prohibited.

12.3.1.2. Securing Premises from Fire

- All computer systems must be housed in an environment equipped with fire extinguishers.
- The fire extinguishers must be placed in such a way so that they are easily accessible in all areas.
- Smoke detectors must be located and within Server Room, which must automatically trigger on the smoke alarm as soon as smoke is detected.
- Fire safety equipment must be checked regularly in accordance with manufacturer's instructions. A maintenance sheet must be maintained with the equipment.
- Hazardous and combustible materials must be stored at a safe distance from server rooms. Computer supplies such as stationery must not be stored in server room.
- Comprehensive fire and emergency instructions must be displayed in prominent locations.

- Functioning and operations of the fire safety devices / equipment installed must be explained to employees of Corporate Services department and security guards periodically during Internal Training Programs.
- Regular mock drills shall be conducted to ensure effectiveness of the training and instructions to be followed in case of fire.
- Securing Premises from Water Hazards
- Computer and communication rooms will not be in areas susceptible to water seepage and flooding like the basement.
- Electrical equipment, damaged due to water, must be checked and dried before being returned to service.

12.4. Power Supplies

12.4.1. Policy Statements

12.4.1.1. Power Supply Controls

- Uninterrupted Power Supply (UPS) must be installed to ensure continuous running of information processing equipment.
- UPS equipment shall be maintained in accordance with the manufacturer's recommendations to ensure that it is in working condition.
- All buildings must be properly earthed to prevent electric surges.
- Voltage regulators must be installed to guard against fluctuations in power. Circuit breakers of appropriate capacity must be installed to protect the hardware against power fluctuations or shot circuits.
- There will be Lightning protection filters for the buildings.

13. Human Resource Management and Personnel Security Policy

13.1. Introduction

Human Resource management and Personnel security must be implemented to address the risks of human error, theft, fraud, or misuse of facilities and assist all personnel in creating a secure computing environment.

An integral part of PremiumTrust Bank's information processing is its user-base, in particular its personnel. Personnel are exposed to information throughout their working day, some of which may be confidential or business critical. The Bank needs to take the necessary steps to ensure that staff hired are trustworthy and perform as required.

The Bank has recognized this pertinent threat and has therefore formulated this Human Resource Management and Personnel Security Policy to address the attendant risk.

13.1 Policy Statement

Personnel security must be implemented to address the risks of human error, theft, fraud, or misuse of facilities and assist all personnel in creating a secure computing environment.

13.1.1 Roles and Responsibilities

Roles and responsibilities of each employee shall be defined and documented. The HR Manager shall ensure that all the employees are aware of their roles and responsibilities.

The People Management Group in consultation with the Chief Information Security Officer shall identify security responsibilities for employee group as per access control classification and explicitly specify the responsibility in the employee job description and responsibility statement. This will include any general responsibilities for implementing or maintaining security policy, legal responsibilities, and rights as well as any specific responsibilities for the protection of particular assets (such as employer's data) or for the

execution of particular security processes or activities, internal or external to the organization.

13.1.2 **Personnel Screening**

The People Management Group in charge of recruitment shall carry out background checks on permanent staff at the time of job applications. This shall include the following:

- Availability of satisfactory character references (One business)
- A check (for completeness and accuracy) of the applicant's curriculum vitae.
- Confirmation of claimed academic and professional qualifications.

A similar screening process shall be carried out for contractors and temporary staff. Where this staff is provided through an agency, the contract with the agency shall clearly specify the agency's responsibilities for screening and the notification procedures they need to follow if screening has not been completed or if the results give cause for doubt or concern. The responsibility for screening contract and temporary personnel shall be carried out by the People Management Group.

13.1.3 **Agreements**

The People Management Group shall include "Confidentiality agreement" and "non-disclosure agreement" as part of the initial terms and conditions of employment for all prospective employees of PremiumTrust Bank Limited.

The People Management Group shall review the "Confidentiality Agreement" periodically when there are changes to terms of employment or contract, particularly when employees are due to leave the organization or contracts are due to end.

Contracts signed by an employee shall include the "terms and conditions of employment". The terms and conditions will include:

- Responsibilities of an individual while working onsite or offsite

- Code of conduct and ethics whilst being employed
- Certain responsibilities to be followed after termination till a defined period
- Actions that will be taken if the employee disregards these contracts

13.1.4 **Information security awareness and training**

- Information and Cybersecurity team shall work with the People Management Group to arrange for appropriate training and awareness sessions on information and cyber security.
- This training shall include subject areas like organizational security requirements, organizational security policies and procedures, cyber security threats and concerns, legal responsibilities and business controls, as well as correct use of information processing facilities e.g., log-on procedure, use of software packages.
- Employees will also be issued alerts whenever required through emails by the respective departments.
- Training programs shall be conducted regularly to make users aware of new security threats and updates in security policies and procedures and attendance logs will be stored of each.

13.1.5 **Job Change and Termination**

The People Management Group in consultation with Information and Cyber Security team will oversee inclusion of appropriate security clauses and procedures in Job Change/Job termination procedures for all employees of PremiumTrust Bank and ensure that appropriate and timely actions are taken so that internal controls and security are not impaired by such occurrences.

The procedures will include but not be limited to:

- Recovery of all documents, issued keys, borrowed IT equipment (e.g., Laptops, data media) and PremiumTrust Bank access cards.
- Revoking/deleting of all entry and access rights held by the departing staff. This includes external access authorizations over data communications equipment. If, in exceptional case, several persons shared access right to an IT system (e.g., by using a common password), the access rights must be altered upon termination of employment by one of those individuals.
- It shall be explained to the departing person that all confidentiality agreements remain in force and that no information obtained in the course of his /her work may be disclosed.
- Update contingency plans if the departing staff member was assigned functions under the plan.

13.1.6 **Disciplinary Actions**

- All violations of the Information Security Policies shall be reported to the respective user Business Head or Chief Information Security Officer.
- Non-compliance with the policies can result in counselling, warnings or disciplinary proceedings extending to termination of service.
- A staggered approach may be followed while implementing the compliance mechanism. Employees may be initially let off with a lighter penalty (e.g., an oral reprimand). However, the actual nature and extent of the action shall be determined by the Management in consultation with the People Management Group in line with PremiumTrust Bank Staff Handbook.

14. Cloud Security Policy

14.1. Introduction

A cloud security policy provides a formal guideline to ensure safe and secure operations in the cloud. These cloud services allow the Bank run services outside the conventional on-premises hardware and IT infrastructure to virtual private or third-party cloud services. Hence, it is imperative to put in place relevant security controls to manage potential security risks.

Cloud Computing involves using a network of remote servers hosted within a private cloud or by a cloud service provider to store, manage and process data. Cloud Computing may involve any of the following categories:

- Infrastructure as a Service
- Software as a Service
- Platform as a Service

Cloud Security is the practice of safeguarding cloud computing environments hosting application, data, and information amongst others.

This policy sets out the Bank's guidelines on the security of cloud computing services.

14.2. Definition of Terms

- ✓ **Infrastructure as a Service (IaaS):** IaaS is a form of cloud computing that provides virtualized computing resources over the internet. In the IaaS model, the cloud provider manages IT infrastructures such as storage, server and networking resources, and delvers them to subscriber organizations via virtual machines accessible through the internet.
- ✓ **Software as a Service (IaaS):** SaaS is a method for delivering software applications over the Internet, on demand and typically on a subscription basis. With SaaS,

cloud providers host and manage the software application and underlying infrastructure, and handle any maintenance, like software upgrades and security patching. Users connect to the application over the Internet, usually with a web browser on their phone, tablet, or PC. Typical examples are email, calendaring, and office tools (Such as Microsoft Office365).

- ✓ **Platform as a Service (PaaS):** PaaS is cloud computing mode that provides platform for customers to develop, run, and manage applications without building and maintain the cloud infrastructure required to develop and launch applications. PaaS is designed to make it easier for developers to quickly create web or mobile apps, without worrying about setting up or managing the underlying infrastructure of servers, storage, network, and databases needed for development.

14.3. Purpose

The purpose is to define the security requirements on the use of cloud services within PremiumTrust Bank. It serves to outline guidelines to protect the confidentiality, integrity and availability of information being processed, stored, or transmitted across cloud services.

14.4. Scope

This policy applies to all PremiumTrust Bank staff, business processes, units, or service providers and third parties with access to cloud services involving PremiumTrust Bank's Information System resources. It shall also apply to all cloud computing services to which the Bank shall subscribe to.

14.5. Policy Statement

The Bank shall subscribe to cloud service providers/vendors, when necessary, in order to gain access to computing resources (servers, and storage), software services, and virtual

application development platforms. This will be done after appropriate risk assessment has been performed and relevant approvals obtained. Access to these cloud services shall be securely managed to ensure that the Bank's information is not compromised while transferring, processing and/or storing information on the cloud platforms.

14.5.1. Policy

- Subscription to cloud service providers shall be subject to Management approval and must be backed by a business case. The Chief Information Security Officer [CISO] and Chief Information Officer (CIO) will certify that security, privacy and all other IT management requirements will be adequately addressed by the cloud services vendor.
- The use of such services must comply with the Bank's existing Acceptable Use Policy.
- Personal cloud service accounts shall not be used for storage, processing, or exchange of the Bank's information.

14.5.2. Risk Assessment

- Prospective cloud service providers shall be thoroughly assessed to ascertain their competence and ensure they comply with relevant security certifications (PCI DSS, ISO, etc.).
- An internal risk assessment and analysis shall be performed on all services to be hosted on the cloud. The assessment shall identify any risks to the Bank, business unit, process, security and/or data stored. Relevant mitigations shall be recommended to address all the concerns raised. The assessment shall be based on ISO 27017 standard and Cloud Security Alliance recommendations.

14.5.3. Service Level Agreement

- For any cloud services that require users to agree to terms of service, such agreements must be reviewed and certified okay by the Legal team.
- All subscriptions to cloud services must be bound by a Service Level Agreement (SLA).
- Every cloud service SLA must have appropriate provisions for security and privacy of the Bank's critical information.
- The cloud service SLA must maintain legal protections for the privacy of data stored and processed on the provider's system.
- Responsibilities over security and privacy shall be clearly addressed in the agreement or contract with the cloud service provider.
- The SLA shall explicitly require cloud service providers to notify the Bank in a timely manner of any occurrence of a breach to the service provider's system, regardless of the parties or the data directly impacted.

14.5.4. Access Control

- Management of user credentials for all cloud services shall be in line with the Bank's Identity and Access Management policy.
- All software development on Platform as a Service (PaaS) solutions shall comply with the Bank's Application Management Policy.
- All Infrastructure as a Service (IaaS) devices shall be configured to meet the requirements outlined in the Bank's System Compliance Policy. The administration of such devices shall comply with the guidelines stipulated in the System Compliance Policy.

- All access to cloud services (including but not limited to access provisioning, access review, access de-provisioning) shall comply with requirements in the Identity and Access Management policy.
- All administrative and privileged accounts for cloud solutions shall require multi-factor authentication before log-on.
- Access to publicly accessible cloud services from within the Bank's network shall be routed through the perimeter firewall while access to the Bank's private cloud infrastructure from an external network shall be routed through a Virtual Private Network (VPN) connection.
- All employee mobile devices with access to cloud services shall comply with the mobile security requirements as stipulated in policy.
- Each cloud solution shall have an application/platform-specific security configuration guide which describes how to implement security settings within the application in order to comply with security standards.
- All data being transmitted, stored or processed by cloud services shall be encrypted with a secure cryptographic algorithm.

14.5.5. Auditing

- Activities on all cloud services and systems shall be logged and reviewed regularly.
- Security logging and event management solutions shall be used to monitor activities on all (critical) services hosted in the cloud environment.
- The Bank shall periodically obtain relevant reports such as SOC2 reports from each cloud solution provider to ascertain that adequate controls to protect data and information assets have been implemented and are operating effectively.

- The Bank must ensure that cloud service providers have measures in place for business continuity in the event of any operational or security related incidents.

14.5.6. Security Monitoring

- Incident reporting and management on cloud services shall be in line with the Bank's Incident Management Policy.
- The cloud services shall be integrated with the security information and event management (SIEM) tool to enable visibility into the activities on cloud services.

14.5.7. Regulatory Compliance

- Use of cloud services must be in line with all relevant laws and regulations (such as Nigeria Data Protection Regulation - NDPR) governing the handling, processing and storage of personally identifiable information, corporate financial data or any other data owned or collected by the Bank.

14.5.8. Exit Procedure

- A comprehensive exit process from the service provider shall be outlined in the SLA which shall include amongst other things, ensuring that the Bank retains all her critical information and that all copies of the Bank's information are permanently erased from the service provider's infrastructure/platform/software/storage.
- An exit (or a discontinuation) from a cloud service shall be initiated by the owner of such service followed by an approval from both the unit head, CIO and the CISO.

14.5.9. Disciplinary Action

Violation of this policy may result in disciplinary action, which may include:

- Termination for employees.
- Termination of employment relations in the case of contractors or consultants.

- Dismissal for interns and volunteers.

Cloud security breach/incidents will be handled in line with the Bank's cyber incident response plan.

15. Electronic Banking Policy

15.1. Objective

The purpose of this policy is to establish guidance on how to identify, measure, monitor, and control risks arising from the use of electronic services. It sets forth the expectations of PremiumTrust Bank Management when implementing and operating E-Business systems.

15.2. Policy Statement:

15.2.1. All PremiumTrust information accessed and/or processed via publicly available systems shall be appropriately protected to ensure its confidentiality, integrity and availability.

15.2.2. Users shall adhere to the guidelines set out in the Information Classification policies and procedures.

15.2.3. Users shall not logon to customers' accounts and execute any transactions.

15.2.4. Users shall not obtain logon credentials from any user.

15.2.5. Users shall log-off/sign-off when they are no longer using e-banking portal/applications.

15.2.6. All electronic banking arrangements between PremiumTrust Bank and its business partners shall be supported by a signed agreement. The agreement will commit both parties to agreed terms of business, such as level of security (i.e., encryption standards), authentication method and authorisation for

transactions and non-disclosure agreements.

15.2.7. Information assets stored or processed using e-banking shall be classified according to their level of sensitivity.

15.2.8. Information will be protected according to its classification.

15.2.9. Information published and accessed through PremiumTrust Bank's Website shall be accurate.

15.2.10. Information and links to other sites from PremiumTrust Bank's website shall be verified for accuracy and functionality.

15.2.11. Standard disclaimer clauses notifying customers that they are leaving PremiumTrust Bank's website (secure environment) shall be maintained for all external links from PremiumTrust Bank's website.

- This clause shall notify the customers that PremiumTrust Bank does not have control or liable over contents outside its website.
- Standard notifications shall be displayed when moving from a secured site (https) to/from unsecured site (http).

15.2.12. Customer's e-Banking platforms (Internet banking, Electronic Payment System) requests shall be routed through firewalls to severs within the PremiumTrust Bank DMZ.

15.2.13. Security perimeters shall be placed between PremiumTrust Bank's WAN/LAN and all external networks including the Internet. All routed connections shall only be made through secure and approved servers located within a DMZ.

15.2.14. Classified information transmitted over public networks shall be properly controlled (through encryption and related techniques) to ensure the confidentiality and integrity of data.

15.2.15. Secure connection protocols (such as HTTPS) and appropriate firewalls shall be used.

15.2.16. PremiumTrust Bank information involved in e-banking shall be protected against incomplete transmission, misrouting, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or relay.

15.2.17. User profiles with unique identifiers and specific access privileges shall be maintained for all e-banking customers.

15.2.18. External threats to electronic banking systems will be mitigated via the use of appropriate techniques. This may include the use of anti-virus software and firewalls that are configured according to PremiumTrust Bank's security standards.

15.2.19. Vulnerability tests, penetration tests and regular reviews to identify breaches of the policies and threats to the e-banking environment shall be performed.

15.2.20. The management of ATM card and PIN issuance shall follow an approved documented process.

15.2.21. ATM cards and PINs shall not be stored or transported together.

15.2.22. The issuance of ATM cards and PINs shall be segregated.

15.2.23. ATM PINs shall be protected from unauthorised access.

15.2.24. Generated ATM PINs shall be encrypted.

15.2.25. Appropriate logical access controls shall be used to control access to the PIN mailer application.

15.2.26. Logs of user activities on the PIN mailer application shall be maintained.

15.2.27. PremiumTrust Bank's Automated Teller Machines (ATM) shall strive to meet

customers' expectation of zero tolerance for downtime.

15.2.28. Daily monitoring of ATM cash and consumable status shall be performed by the responsible operations and E-Business staff.

15.2.29. ATM availability shall be monitored and reported.

15.2.30. Customers shall be made aware of the need to keep their PINs secret and cards safe.

15.2.31. Customers will not have the ability to unwittingly provide authorisation information to third parties.

15.2.32. Two-factor authentication shall be applied at a minimum for processing transaction to all internet banking services.

15.2.33. E-banking customers and partners shall be forced to use strong passwords by implementing appropriate security settings for all production applications.

15.2.34. E-banking transactions shall be logged and properly kept in line with legal and business requirements. Logs of e-banking transactions shall be tamper-proof.

15.2.35. All ATM transactions shall be reconciled on daily basis.

15.2.36. Open items on ATM reconciliation shall be resolved in line with the approved procedure.

15.2.37. Reference(s)

i. Identity and Access Management Policy

16. Bring Your Own Device (BYOD)

16.1. Objective

The purpose of this policy is to protect PremiumTrust Bank's, data and systems from being deliberately or inadvertently exposed, lost, disclosed, altered or manipulated, while enabling authorized persons to access PremiumTrust's network and systems using their devices. This policy sets out the circumstances in which IT may monitor authorized persons' connection to PremiumTrust Bank's network, access their devices and retrieve, remove, or destroy data on it and the action to be taken in respect of breaches of this policy.

16.2. Scope

- This policy applies to staff of PremiumTrust Bank who use personal mobile devices which include but are not Limited to any accompanying software or hardware (hereinafter referred to as 'a device' or "personal device") to access PremiumTrust Bank's Data. It applies to the use of the device both during and outside office hours and whether use of the device takes place at the normal place of work.
- This policy applies to all devices used to access PremiumTrust Bank's Resources which for this purpose may include but are not Limited to Smartphones, mobile or cellular phones, Personal Digital Assistants (PDAs), tablets, and laptop or notebook computers.

16.3. Policy

16.3.1. General Requirement

16.3.1.1. The use of any personal mobile device or other device covered by this policy is subject to written acceptance and strict adherence to the terms and conditions of this Policy.

16.3.1.2. No staff shall be compelled to use their personal mobile device for PremiumTrust Bank's business purposes. It is a matter entirely at the staff's discretion and the Approval of designated authorities within PremiumTrust Bank

16.3.1.3. Certain obligations under this policy are contractual and impact on the Employee's contract of employment. PremiumTrust Bank's may vary, alter, or amend this policy, including the contractual obligations that it places on staff.

16.3.1.4. Breach of this policy may lead to PremiumTrust Bank's revoking an authorized person's access to PremiumTrust Bank's systems, whether through a device or otherwise. It may also result in disciplinary action which may lead to the dismissal of the affected staff, and in the case of a breach of this policy by a contractor, consultant, casual or other agent of PremiumTrust Bank, (the automatic termination of engagement in addition to the other sanctions specified in the applicable contract for services with the affected agent. Disciplinary action may be taken irrespective of whether the breach is committed during or outside office hours and whether use of the device takes place at the normal place of work. Such Holder or authorized persons are required to cooperate with any investigation into suspected breach, which may involve providing PremiumTrust Bank with access to the device and any relevant passwords and login details.

16.3.1.5. Some devices may not have the capability to connect to PremiumTrust Bank's systems. PremiumTrust Bank is not under any obligation to modify PremiumTrust Bank's systems or otherwise assist staff or Holder in connecting to PremiumTrust Bank's systems.

16.3.2. Connecting Devices to PremiumTrust Bank's Systems

16.3.2.1. Connectivity of all devices is centrally managed by Information and Cyber Security Group who must approve a device before it can be connected to PremiumTrust Bank's systems. A device must be on the approved list of devices, available with Information Technology (IT) Department and approved by Chief Information Security Officer (CISO).

16.3.2.2. It is the collective responsibility of both Information and Cyber Security Group and IT to provide PremiumTrust Bank, its Staff and partners with a comprehensive list of acceptable devices which must be submitted to the relevant stakeholders for necessary approval prior to publication. The approved list of devices will take into consideration acceptable devices and operating system versions that are adaptable to PremiumTrust Bank's IT infrastructure.

16.3.2.3. PremiumTrust Bank reserves the right to refuse permission or to disconnect a device from PremiumTrust Bank's systems. IT Department shall refuse or revoke such permission (and may take all steps reasonably necessary to do so) where in its reasonable opinion, a device is being or could be used in a way that puts, or could put PremiumTrust Bank's systems, data, staff, or business connections at risk or that may otherwise breach this policy.

16.3.2.4. Prior to connection to PremiumTrust Bank's network, all personally owned, and PremiumTrust Bank issued devices shall pass through a formal enrolment process. This implies that devices shall be profiled. For example, it may be necessary to change configuration setting or install new applications. Authorized persons should note that when these modifications are tampered with, access to PremiumTrust Bank's networks will be disabled immediately.

16.3.3. Management, Control and Monitoring

16.3.3.1. Device Management

- All PremiumTrust Bank's data stored either on its devices or personal devices remain PremiumTrust Bank's property. All materials, data, communications, and information, including but not Limited to e-mail (both outgoing and incoming), telephone conversations and voicemail recordings, instant messages and internet and social media postings and activities, created on, transmitted to, received or printed from, or stored or recorded on a device during business or on our behalf of PremiumTrust Bank belongs to PremiumTrust Bank regardless of who owns or uses the device.
- PremiumTrust Bank reserves the right to monitor, intercept, review, and erase, without further notice, all content on the device that has been created on behalf of PremiumTrust Bank. This includes without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, logins, recordings and other uses of the device [as well as keystroke capturing and other network monitoring technologies], whether or not the device is in your possession.
- Therefore, authorized persons should have no expectation of absolute privacy in any data belonging to PremiumTrust Bank which is stored on the device.
- Monitoring, intercepting, reviewing, or erasing of content will only be carried out to the extent permitted by law, for legitimate business purposes, including, without limitation, to:
  a) Prevent misuse of the device and protect PremiumTrust Bank's data;
  b) Ensure compliance with PremiumTrust Bank's rules, standards of conduct and policies in force from time to time (including this policy);
  c) Monitor performance at work; and

d) Ensure that staff members do not use PremiumTrust Bank's facilities or systems for any unlawful purposes or activities that may damage PremiumTrust Bank's business or reputation.

- PremiumTrust Bank may also store copies of any content for a period of time after they are created and may delete such copies from time to time without notice. PremiumTrust Bank may obtain and disclose copies of such content or of the entire device (including personal content) for litigation or other investigations.
- All authorized persons are also hereby deemed to agree that they use the device at their own risk and that PremiumTrust Bank will not be responsible for any losses, damages or liability arising out of its use, including any loss, corruption or misuse of any content or loss of access to or misuse of any device, its software or functionality.

16.3.3.2. Security Requirements

- Authorized persons must comply with PremiumTrust Bank's Information security policy when using a device to connect to PremiumTrust Bank's systems.
- In addition, and to the extent that this Policy does not address the issues below, Staff must:

a) At all times, use best efforts to physically secure the device against loss, theft or use by persons who are not authorized to use the device. Staff must secure the device whether it is in use and whether it is being carried or held by staff at any point in time.

b) Employ the use of passwords, encryption, and other control mechanisms to protect the devices.

c) Install anti-virus or anti-malware software as required by PremiumTrust Bank before connecting to PremiumTrust Bank's systems and must also co-operate with IT Department in its efforts to ensure the safety and security of PremiumTrust Bank's data which are stored in the device(s) which include, providing us with any necessary passwords when requested.

d) Comply with the device configuration requirements as advised by IT.

e) Protect the device with a PIN or password and always keep that PIN or password secure. The pin number or password should be changed every 3 months. If the confidentiality of a pin number or password is compromised, have it change immediately. However, the use of pin numbers and passwords should not create an expectation of absolute or unqualified privacy by staff in the device.

f) Maintain the device's original operating system and keep it current with security patches and updates.

g) Not download and install software to the device unless explicitly authorized by PremiumTrust Bank. A list of applications that are already authorized and those that are expressly forbidden is available with IT Department

h) Not alter the security settings of the device without IT Department's consent.

i) Prohibit use of the device by persons not authorized by PremiumTrust Bank, including family, friends and business associates.

j) Not download or transfer any PremiumTrust Bank's confidential data to the device, for example via e-mail attachments, unless specifically authorized to do so. Staff must immediately erase any such information that is inadvertently downloaded to the device.

k) Not backup the device locally or to cloud-based storage or services where that might result in the backup or storage of PremiumTrust Bank's data. Any such backups inadvertently created must be deleted immediately

l) Not use a device to capture images, video, or audio, whether native to the device or through third-party applications, within the workplace.

m) Where PremiumTrust Bank has permitted or authorized the transfer or storage of PremiumTrust Bank's data on the device, ensure that the PremiumTrust Bank's data is encrypted using appropriate encryption technologies.

n) Not use the device as a mobile hotspot without consent from IT Department and Information and Cyber Security Group.

o) Shall not connect the device to an unknown Wi-Fi.

- PremiumTrust Bank reserves the right among others to:

  a) Inspect the device for use of unauthorized applications or software.

  b) Inspect any PremiumTrust Bank's data stored on the device or on backup or cloud-based storage applications and prevent misuse of the device and protect PremiumTrust Bank's data.

  c) Investigate or resolve any security incident or unauthorized use of PremiumTrust Bank's systems.

  d) Conduct any relevant compliance obligations (including in relation to concerns regarding confidentiality, data protection or privacy); and

  e) Ensure compliance with PremiumTrust Bank's rules, standards of conduct and policies in force from time to time (including this policy).

  - If the PremiumTrust Bank discovers or reasonably suspect that there has been a breach of this policy, including any of the security requirements listed above, PremiumTrust Bank shall immediately withdraw access to its systems and, where appropriate, remove any PremiumTrust Bank's data from the device. Although PremiumTrust Bank does not intend to wipe other data that is personal in nature (such as photographs or personal files or e-mails), it may not be possible to distinguish all such information from PremiumTrust Bank's data in all circumstances, you should therefore regularly backup any personal data contained on the device.
  - Authorized Person must co-operate with PremiumTrust Bank to enable such inspection, access and review, including providing any passwords or pin numbers necessary to access the device or relevant applications. A failure to co-operate with us in this way may result in disciplinary action being taken, up to and including dismissal. This paragraph of the policy is contractual.
  - PremiumTrust Bank will not track any personal devices via GPS or location-based Wi-Fi without the staff or the device owner's permission.

16.3.3.3. Lost or Stolen Devices and Unauthorised Access

- In the event of a lost or stolen device, or where a staff member or Authorized Person believes that a device may have been accessed by an unauthorized person or otherwise compromised, the staff member or Authorized Person must report the incident to Information and Cyber Security Group and IT following the incident reporting procedure.
- Appropriate steps will be taken to ensure that PremiumTrust Bank's data on or accessible from the device is secured, including remote wiping of the device where appropriate. The remote wipe will destroy all PremiumTrust Bank's data on the device (including information contained in a work e-mail account, even if such e-mails are personal in nature).

Although PremiumTrust Bank does not intend to wipe other data that is strictly personal in nature (such as photographs or personal files or e-mails), it may not be possible to distinguish all such information from PremiumTrust Bank's data in all circumstances, Authorized Person should therefore regularly backup all personal data stored on the device.

16.3.3.4. Termination of Employment

Upon Employees or authorized person's exit from PremiumTrust Bank's employment or contract, Employee or other Authorized Person agrees to IT Department's removal of all PremiumTrust Bank's data (including work e-mails), and any software applications from the device. Where the data cannot be remotely removed, the device must be submitted to IT Department for relevant wiping of data and software removal. Employees or

Authorized person also hereby undertakes to co-operate with IT Department in this process as failure to do so may attract sanctions including but not Limited to PremiumTrust Bank exercising rights over the Employee or other Authorized person's entitlements with PremiumTrust Bank.

16.3.4. Personal Data

PremiumTrust Bank shall use reasonable endeavours not to access, copy or use any personal data held on the device without the permission from the owner of the personal data. If such access or copying occurs inadvertently, PremiumTrust Bank shall delete any and all such personal data as soon as it comes to its attention. This limitation does not apply to personal data which is also PremiumTrust Bank's data (including personal e-mails sent or received using PremiumTrust Bank's e-mail infrastructure). For this reason, Staff are encouraged not to use work e-mail for personal purposes.

I. **Appropriate Use**

- Before using a personal device under this policy for the first time, Authorized person must erase all information and software related to any previous employment. Authorized person must confirm to PremiumTrust Bank that this has been done if asked to do so.
- Authorized person should never access PremiumTrust Bank's data or use PremiumTrust Bank's systems in a way that breaches any of PremiumTrust Bank's policies. Importantly, Authorized person must not use a device to:
    - Breach PremiumTrust Bank's obligations with respect to the rules of relevant regulatory bodies.
    - Breach any obligations that relevant regulatory bodies may have relating to confidentiality and privacy.
    - Defame or criticize PremiumTrust Bank, its affiliates, customers, clients,

business partners, suppliers, vendors, or other stakeholders.

- Harass or bully other staff in any way
- Breach any other laws or ethical standards (for example, by breaching copyright or licensing restrictions by unlawfully downloading software on to a device).

- A breach of any of the above policies attracts disciplinary action up to and including dismissal.
- Authorized persons must not, make or receive voice calls without the use of appropriate hands-free devices, text, e-mail or otherwise use a device while operating a company vehicle or while operating a personal vehicle for business purposes. Authorized persons must comply with any applicable law concerning the use of devices in vehicles. For own safety and the safety of others, PremiumTrust Bank recommends that Authorized Persons should not use a device while operating vehicles of any kind.

II. Technical Support

PremiumTrust Bank does not provide technical support for devices. If Employee uses a device for business purposes, Employee will be responsible for any repairs, maintenance or replacement costs and services. However, if there is an issue with the device relating to software provided by PremiumTrust Bank, then PremiumTrust Bank' will provide any necessary support.

III. Costs and Reimbursements

Employee must pay for own device costs under this policy, including but not Limited to voice and data usage charges and any purchase and repair costs. By signing the

Information security declaration Employee acknowledges responsibility for all costs associated with the device and that business usage of the device may increase voice and data usage charges.

16.3.5. Persons Responsible for this Policy

- PremiumTrust Bank's Board of Directors have full responsibility for the effective operation of this policy but has delegated the obligation for its day-to-day operation, implementation, and administration to the Chief Information Security Officer (CISO)
- The CISO has responsibility for ensuring that any person who will be involved with administration, monitoring, IT security or investigations out under this policy receives regular, appropriate, and up to date training to assist them with these duties.
- All staff shall be responsible for the success of this policy. Any misuse (or suspected misuse) of a device or breach of this policy should be reported.
- Any questions regarding this policy implementation or the usage of devices for business purposes which are not addressed in this policy should be directed to the CISO.

16.3.6. Reference(s)

i Identity and Access Management Policy

ii Network Management Policy