Allied Bank

“Information Security Policy”

Version 4.0

CONFIDENTIAL MATERIAL – FOR BANK’S USE ONLY

RECOMMENDATION & REVIEW

RECOMMENDED FOR APPROVAL

Chief RMG

REVIEWED BY

Chief RBG	Chief CBG
Chief IBG	Chief CIBG
Chief SAMG	Chief ITG
Chief Treasury	Chief HRG
Chief BSG	Chief GS&SG
Chief FG	Chief CAG
Chief CG	CEO

PUT UP IN BOD MEETING NO 233

Date 9-8-18 Initial

Put up in RMC Circulation/

Meeting No. 6

Dated: 12-6-18 Item No. 11

PUT UP IN BRMC MEETING NO 61

Date 19/7/18 Initial

RMC

BRMC

PUT UP IN BOD MEETING NO 233

Date 9-8-18 Initial

Put up in RMC ~~Circulation /~~

Meeting No......6......

Dated:..28-6-18..Item No......11......

PUT UP IN BRMC MEETING NO 61

Date 19/7/18 Initial

Document Description

Title	Information Security Policy v4.0
Ownership	Information Security & Governance - RMG
Approving Authority	Board of Directors
Date of Approval	
Document Type	Full Policy review
Date of Implementation	
Review Frequency	03 years or as and when required *Policy will remain valid till next approval*
Last Approval Date	25-04-2014
Next Review Date	At least after 03 years of approval date
Accessibility	ABL Portal

CONTENTS

1 OBJECTIVE OF INFORMATION SECURITY POLICY

1.1 INTRODUCTION

The Information Security Policy is a document made initially as per ref: **SBP BSD Circular No. 03 of 2007 dated: April 04, 2007** that dictates Information Security scope, objectives, assigns roles and responsibilities. It provides a direction required for mitigating risks to information stored, processed, and/or transmitted. It also helps protect Bank by communicating priorities, and exercising "Due Diligence". Subsequently this document is revised based upon "***Enterprise Technology Governance & Risk Management Framework for Financial Institutions***" Issued vide BPRD Circular No. 05 dated May 30, 2017 and "***PCI DSS v3.2 April 2016"***. The Information Security Policy illuminates the importance of security, and details how the security policy will be implemented and enforced. The policy requires compliance in line with regulatory and statutory requirements related to the Bank information and information processing resources, including applications, networks, systems, infrastructure and storage.

1.2 OBJECTIVE

Information Security Policy objective is to safeguard the Bank's Information Assets.

1.3 MANAGEMENT COMMITMENT

Bank Management shows its commitment towards implementing ISM by doing the following:

1. Establishing ISM objectives and plans as per business objective and regulatory requirements.
2. Establishing roles and responsibilities for ISM.
3. Maintaining Information Security Policy.
4. Establishing the information security forum within Bank and regularly reviewing the group's performance against the set ISM objectives.
5. Providing sufficient resources to establish, implement, operate, monitor, review, maintain and improve the ISM.
6. Ensuring the development of Information Security Team, keeping them abreast with latest Information/Cyber risk management trends and techniques in order to counter existing and new forms of cyber threats. (ETG&RMF 2.9 (e))
7. Monitor technological developments and keep abreast with new cyber risk management processes that can effectively counter existing and new forms of cyber threats. (ETG&RMF 2.9 (e))
8. Ensuring that Internal Information Security Audits are conducted.
9. Establishing information security procedures that support effective implementation of Information Security Policy. Mandatory procedures shall be established by the respective functions.
10. Establishing criteria for accepting information security risks and threats.
11. Conducting management reviews of the ISM once in a year.

2 SCOPE AND IMPLEMENTATION

1. Information Security Policy applies to all Bank Offices, employees, consultants and external parties.
2. This policy covers the usage of all of the Bank's information technology and communication resources, whether owned or leased, including:
   a) All computer-related equipment, including desktop PCs, portable PCs, terminals, laptops, smart phone, tablets, wireless computing devices, printers, servers, authentication devices, ATMs etc.
   b) All data and software residing on the Bank-owned equipment.
   c) Information security policy also applies to all users, whether on the Bank's premises or those that connect remotely via network connection including the ones using its information processing equipment
3. All functions are responsible to formulate relevant procedures, guidelines, baselines and standards to ensure effective implementation of Information Security Policy across Bank.

2.1 RIGHTS OF INSPECTION

Information security division in the absence of SIEM implementation with particular log source, with mutual consents has the right to inspect the logs at any time or may ask to show the same with reference to any system/application/device or an individual in question for a specified time period.

2.2 ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary action, as per HR Group Policies and possible civil and/or criminal prosecution to the full extent of law.

2.3 POLICY EXCEPTION

Any exception to Information Security Policy must be approved by CEO of the Bank on the recommendation of Chief ITG and Chief RMG, on the proposal comprising the acceptance of associated risk(s) by Group Chief concerned and recommendation of GH Information Security & Governance. Please refer **Annexure A** "Risk Acceptance by Clause(s) Exception Form".

3 ROLES, RESPONSIBILITIES & AUTHORITIES

3.1 INFORMATION SECURITY & GOVERNANCE - RMG

1. Develop Information Security Policies and its related procedures in coordination with relevant stakeholder and arrange approval.
2. Strengthen Information Security in coordination with ITG to document controls implemented for securing information assets of the Bank.
3. Review/update information security policy and InfoSec's procedures wherever appropriate based upon the following:
   a) Audit recommendations
   b) Input received from Compliance, ITG, and any other internal business group
   c) Regulatory requirements
   d) Best practices as per Bank's environment
   e) Any other event
   f) Disaster Recovery Plan
   g) Business Continuity Plan
4. Conduct Technical Risk Assessment (TRA) exercise and maintain Risk Register of all information assets held by the Bank.
5. Plan, perform, and review vulnerability scanning and Penetration Testing.
6. Engage available external consultants having sufficient relevant expertise in Information Security Assessment and Penetration Testing.
7. Develop SOC (Security Operation Center) to:
   a) Develop and maintain capability to effectively monitor available logs to identify and report Information Security Incidents
   b) Analyze reported incidents and give recommendations to ensure that exposures of incidents are contained and recovery achieved within specified timelines
8. Monitor, analyze, and report ICT Infrastructure with respect to Information Security events, coordinate and escalate issues to concerned functions.
9. Providing InfoSec related feedback/evaluation while acquiring or development of any new systems/software as and when required by relevant stakeholder.
10. Devise Information Security Awareness campaign for the Bank in liaison with HRG.
11. RMG shall develop Bank's Cyber Security roadmap in coordination with relevant stakeholders and monitor its implementation. Moreover, ensure periodical reporting of cyber-attacks that cause disruption of customer information, critical banking services etc. to Bank's Senior Management and share with all relevant stakeholders.

3.2 INFORMATION TECHNOLOGY GROUP

1. Develop its policies, procedures, and guidelines in line with Bank's Information Security Policy, where applicable.
2. Implement effective IT Security Controls & Risk Mitigation measures over Software, Applications,

Information, Data, Networks, Servers & Data Center as per regulatory and Bank's policies and procedures.

3. Develop Technical Risk Treatment Plan on the basis of outcomes of TRA exercise.
4. Maintain a list of B2B partners and ensure adequate security measures have been taken while establishing electronic relation.
5. Ensure and maintain status that service provider is compliant with PCI-DSS requirements where applicable, and Bank's Information Security policy.
6. Monitor and review respective logs for operational anomalies policies violations.
7. Develop procedures for Services Delivery, Operations Management, Acquisition, Development & Implementation of technology solutions/systems.
8. Establish and develop Project management function for IT Projects.

3.3 TECHNOLOGY COMPLIANCE — CG

Roles and responsibilities are attached in **"Annexure B"**.

3.4 HUMAN RESOURCE GROUP - HRG

1. The HRG is responsible for tracking employee participation in the security awareness program.
2. Facilitate the participation in information security awareness program upon hire or need basis and at least annually.
3. Ensuring that employees acknowledgement for Bank's information security policy.

3.5 IT STEERING COMMITTEE (ITSC)

1. Bank shall formulate ITSC with senior officials from different functions including IT, information security, risk management, compliance, operations and business segments.
2. ITSC shall periodically inform BoD on the latest developments on cyber security action plan, its implementation status, a summary report on major threats, attacks faced by the Bank and their estimated impact on its operations. (ETG&RMF 1.4.2 (d))
3. ITSC shall review significant Information/Cyber Security incidents upon submission on regular basis.
4. ITSC shall review and determine the adequacy of the bank's training plan including information/cyber security training for the staff. (ETG&RMF 1.5.2)
5. ITSC shall report Information/Cyber Security related matter to the relevant board committee for their review. (ETG&RMF 1.5.1 (e))

3.6 GENERAL SERVICES & SECURITY GROUP (GS&SG)

1. Ensure physical access controls must be maintained in such a way to avoid unauthorized access or view.

4 POLICY STATEMENTS

4.1 SECURE USE

4.1.1SECURE USE OF WORKSTATION/LAPTOP

1. Only Bank owned and authorized devices are allowed to access corporate networks, data and systems.
2. Access to 3rd party shall be provided in a controlled environment.
3. Physical access control must be maintained in such a way to avoid unauthorized access or view.
4. To maximize the logical security all IT devices must be password protected as per the requirements stipulated in **Section 4.2 'Password'**, where the operating system permits.
5. Bank owned Anti-virus software shall be installed and updated on all workstations/Laptops connecting to corporate network.
6. If due to valid business justification, Anti-virus software is not installed, it shall be periodically evaluated against the latest malware threats.
7. When the user is leaving his/her desktop/ laptop, he/she must lock the laptop/desktop before leaving the desk.
8. Laptop/desktop shall be configured to be locked automatically after maximum of 15 minutes of inactivity, where operating systems permit.
9. All downloaded material must be scanned through Anti-Virus prior to its first run/use.
10. It is the user's responsibility to ensure that any official data residing on his/her workstation is adequately protected by Bank's policies and procedures from unauthorized disclosure and modification.
11. All incidents that constitute a loss of Bank's hardware/Software must be reported to line manager for necessary action.
12. Only licensed software shall be installed.
13. Users are not allowed to download or install any unauthorized or pirated Software/Application.
14. Usage of USB data storage devices shall be allowed only upon authorization.
15. Sensitive data shall not be stored on personal devices

4.1.2SECURE USE OF INTERNET

1. Internet services provided by Bank must be used ethically.
2. Downloading for other than official purpose from the internet shall be prohibited. However, this privilege can be given based on the individual request which needs to be authorized by the management.
3. Any intentional act causes interruption of official work of Bank and or Staff is strictly prohibited. Any case if found shall be dealt with the disciplinary process as per Bank's HR Policies.
4. Connectivity to the Internet for any purpose through unofficial mechanism shall be strictly prohibited.

4.1.3SECURE USE OF INFORMATION

1. Measures shall be taken to protect information from unauthorized modification, destruction, or disclosure, whether accidental or intentional.
2. Only data or files which have been authorized shall be accessed and any unauthorized attempt to make changes in the privileges of other data or files by any means shall be considered as illegal act.

3. Exchanging information about business partner and their clients or any Bank's confidential information is prohibited unless authorized by concerned competent authority.

4.1.4SECURE USE OF E-MAIL

1. Use of email by employees of Bank is allowed for carrying out official activities only.
2. Any unethical communication through emails is strictly prohibited as per HR Code of Ethics.
   a) User must avoid distribution, dissemination or storage of images, text or materials that might be considered indecent, pornographic, obscene, including offensive comments against cast, creed, race, gender, disabilities, age, religious beliefs and practice, political/ethnic background
   b) Official email address shall not be used to post messages on blogs/ newsgroups etc.
3. Bank reserves the rights to access staff email accounts in the pursuit of an appropriately authorized legal or disciplinary investigation whenever required.
4. For the purpose of clear identification of the originator, email signature shall be present at the end of each outgoing email.
5. The following disclaimer shall be added at server end. The mail server administrator shall verify that emails passing through email server shall have following "disclaimer" in all emails sent outside of the Bank domain:
   "*The contents of this email and any files attached thereto are intended only for the above-named recipient(s) and are confidential and proprietary to Bank. If they have come to you in error, you must take no action based on them. No part of this material shall be reproduced, published in any form by any means, electronic or mechanical including photocopy or any information storage or retrieval system nor shall the material be disclosed to external parties*".
6. E-mail attachments which appear dubious or suspicious must not be clicked/ opened.
7. Creating or forwarding "chain letters" or other pyramid schemes of any type are strictly prohibited.
8. Facility to send e-mail outside of Bank's domain will be given to authorized employees only. Users must exercise maximum caution when forwarding any email from Bank's network to an outside network.
9. Precaution measures shall be taken prior to sending classified document over the email.

4.2 PASSWORD

1. All system-level passwords (e.g., root, enable, windows admin, application administration accounts, etc.) shall be changed before its expiry.
2. All user-level passwords shall be changed at least once in 42 days.
3. Password shall be communicated to users in secure manner.
4. One-time password shall be communicated to end user which shall be changed upon first login attempt where application supports.
5. Where Simple Network Management Protocol (SNMP) is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system".
6. Users must not share his/her password with any user.
7. Passwords shall not be stored by user in clear text on the computer system.

8. In order to get the access of any system of user along with the unique user id, password is also required; password shall meet the complexity requirement with the following criteria where applications/systems/equipment permit:
   a) At least eight characters’ long for normal users and shall be at least 15 characters long for privilege users
   b) Must not be repeated from last 7 passwords
   c) Must not contain user ID, sign on name and user name
   d) Must not be default vendors supplied passwords and shall not be easily guessable
   e) Contains at least 3 of the following 4-character groups
      i. English upper-case characters (A-Z)
      ii. English lower-case characters (a-z)
      iii. Numbers (0-9)
      iv. Non-alphabetic characters e.g. (! @#$%^&*()_+|~-=\`{}[]:";'<>?,./)
9. All login accounts of valid and authorized users not changing their passwords within 90 days for normal user and 45 days for administrative user must be disabled automatically.
10. Password reset requests shall be validated before authentication credential is modified.
11. Service accounts where systems/machines logs into another system are exempted from this policy.

4.3 STORAGE AND RELEASE OF HIGH PRIVILEGE USER IDS

1. Power User ID’s must be securely stored in a dual control safe to prevent disclosure.
2. In case of an emergency/ disaster, the system personnel shall take the appropriate permission from the Chief ITG or Second Authorized Personnel whoever is available first on available media like WhatsApp, telephone or fax. After resolving the emergency, a formal approval shall be taken from Chief Information Technology Group.
3. In case of an emergency/disaster, access to the privileged accounts shall be controlled and monitored. Password of privileged account shall be changed after used.
4. In case of separation of employees who are using power user IDs, the IDs must be disabled immediately and all records must be updated. In case of service account which cannot be disabled, the password of that account shall be immediately changed and all records shall be updated.

4.4 ACCESS CONTROL

4.4.1GENERAL ACCESS CONTROL

1. Access for all systems shall be deny-all except specifically permitted.
2. Access shall be granted and documented only on non-conflicting role based, least privileges and Need-to-know basis and shall be recommended by Functional Head and authorized by Group Head/ Chief.
3. User account’s IDs must not be re-issued to other individuals, consultants and external parties.
4. Temporary user accounts shall be time bound and shall be deactivated when not required.
5. Generic users or group user IDs shall not be permitted. All such IDs shall be deactivated or disabled.

6. Shared user IDs shall not be created / used for system administration activities and other critical functions.
7. Privileged access rights shall be reviewed by line managers at least annually.
8. Default Systems/Applications/Databases. IDs shall not be used for the administration of any system component, where system permits.
9. It is the Line Manager's responsibility to initiate request for granting/revoking/modifying of his/her subordinate's access rights especially in case of transfer, role change, promotion etc.
10. All default and guest accounts on any network device/server/application shall be disabled by respective function administrators where application and its functionality permit.
11. Access for remote users shall be subject to authorization by concerned department and shall be provided in accordance with the **Section 4.5** 'Remote Access'.
12. Unrestricted external access shall not be permitted to any network device or networked system and Bank shall continuously track such actions.
13. Access to storage and media shall be controlled and monitored.
14. Access to data shall be controlled.
15. Appropriate controls shall be implemented to allow access to the vendors on sensitive data/information and systems
16. All User IDs of terminated/separated staff shall be immediately disabled or deactivated as per official intimation from HRG to concerned function.
17. Inactive user accounts shall be reviewed at least every 90 days by respective Application & System owner. Necessary actions shall be taken to remove or disable all such accounts.
18. The User ID shall be locked out after maximum 06 consecutive unsuccessful attempts. Locked out user accounts shall be disabled for a minimum period of 30 minutes or until the administrator enables the account where application/operating system/device OS support this feature.

4.4.2ACCESS TO SENSITIVE CARDHOLDER DATA

1. Access to sensitive cardholder information shall be controlled and authorized. Any Job functions that require access to cardholder data shall be clearly defined.
2. The User ID shall be locked out after maximum 06 consecutive unsuccessful attempts. Locked out user accounts shall be disabled for a minimum period of 30 minutes or until the administrator enables the account. [PCI DSS v3.2, clause 8.1.6, 8.1.7].
3. PAN (Primary Account Number) shall be masked when displayed (first 6 and last 4 digits are maximum digits) unless absolutely unavoidable with legitimated business need.
4. List of Services Providers including a description of the service provided (including 3rd party) shall be maintained to whom cardholder data need be shared. [PCI-DSS v3.2, clause 12.8.1]
5. If Cardholder data is being shared with service provider, a written agreement with acknowledgement (That Service Provider is receiving sensitive Cardholder Information) shall be made to ensure that Service Provider shall maintain all applicable PCI DSS requirements to the extent the service provider handle the Cardholder data. [PCI-DSS v3.2, clause 12.8.2][PCI-DSS v3.2, clause 12.8.2]

6. It shall be ensured that a due diligence is conducted prior to engagement of service provider. [PCI-DSS v3.2, clause 12.8.3]
7. PCI DSS compliance status of the Service provider with whom Bank shares the Cardholders data shall be monitored. [PCI-DSS v3.2, clause 12.8.4]
8. Cardholder's sensitive data shall be encrypted during transmission. [PCI-DSS v3.2, clause 4.1]
9. Ensure all 3rd parties who have access to Cardholder information shall:
   a) Adhere to the PCI DSS security requirements as mentioned above
   b) Acknowledge their responsibility for securing the Cardholder data
   c) Acknowledge that the Cardholder data must only be used for authorized purposes (assisting the completion of a transaction)
   d) Have appropriate provisions for business continuity in the event of a major disruption, disaster or failure
   e) Provide full support and access to conduct a thorough security review on Bank and regulatory instructions. [PCI-DSS v3.2, clause 12.8]
10. Access to CHD shall be role based and shall not be accessed directly except database administrators.
11. Access to CHD shall be controlled and monitored.

4.5 REMOTE ACCESS

1. It is the responsibility of ITG to ensure that Bank employees, contractors, and vendors requesting for remote access privileges to Bank corporate network are given the same security considerations as the user's on-site connection to Bank.
2. In case of VPN, VPN form shall be dully filled and approved from respective department GH and GH-Information Security & Governance.
3. Indemnity bond shall be signed by 3rd party official representative along with technical resource.
4. Remote access shall be strictly controlled and monitored.
5. Strong authentication/Two Factor authentication shall be used to access Bank's resources/Cardholder/Sensitive data.
6. Remote access shall be through secure channels.
7. All idle sessions shall be deactivated/disconnected automatically after 15 minutes of inactivity or as per business need.
8. Vendor and 3rd party remote access accounts shall be enabled or activated for specified time period and shall be deactivated/disabled after the completion of the activity or time period whichever is earlier upon intimation of concerned group/function.
9. All remote access accounts used by vendors or 3rd parties shall be reviewed at regular interval. Any discrepancy shall be documented and necessary actions shall be taken to ensure compliance with regulatory requirements and Bank's policies/procedures.

4.6 CLEAR DESK AND CLEAR SCREEN POLICY

1. All Bank employees in case of sitting in open space are required to clear their desk at the end of their working day or when leaving office premises, whichever is earlier. This includes documents, notes,

business cards and removable media which shall be securely placed. Employees sitting in the rooms with door and lock facility shall lock the room at end of the working day.

2. Employee shall lock their computers when leaving their desk and to log off when leaving for an extended period of time.

4.7 PERSONAL DATA PROTECTION

1. The installed anti-virus software must be kept up-to-date. Virus-infected computers must be removed /disconnected from the LAN until they are verified as virus free.
2. Personal firewall software or equivalent functionality shall be appropriately configured and active on all computing devices that are used to access the CDE. (PCI-DSS 4.1)
3. End user shall not be able to alter the configuration of personal firewall or equivalent functionality software.
4. Information/Data exchange shall be protected in accordance with the requirements of **Section 4.24 'Information Exchange'**.
5. Use of removable media (such as Flash drives, CD-ROMs etc.) shall be strictly controlled.
6. Appropriate controls and tracing through logs shall be available for all systems to monitor activities of privileged users.

4.8 MOBILE DEVICE SECURITY

1. Prior to initial use on the corporate network or related infrastructure, all mobile devices shall be security cleared and shall be registered with ITG.
2. System shall maintain record of all approved mobile devices connecting/accessing the network and information.
3. Mobile devices and their OS versions shall be allowed according to their security strength.
4. All mobile devices shall be password/passcode protected.
5. Devices shall not be "jail-broken or rooted" or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.
6. Antivirus/Anti-Malware shall be installed on all mobile devices which are connected to Bank's network.
7. Any instance of loss or theft of a mobile device shall be reported immediately to the line manager and concerned departments.
8. Any official data residing on mobile devices shall be the responsibility of the user.
9. All incidents that constitute a loss of hardware, data/information, or breach of information shall also be reported to InfoSec through line manager.
10. This policy applies to all mobile devices that have access to corporate networks, data and systems, not including corporate IT-managed laptops. This includes smart phones and tablet computers.

4.9 DATA BACKUP SECURITY

1. The electronic information and related systems shall be backed up, so in the event of any emergency the essential information can be restored successfully.

2. The backup of data, application, configuration, email, and logs shall be maintained securely as per business and regulatory requirements.
3. Onsite/Offsite backup shall be scheduled according to business need, backup archiving and offsite backup movement to DR shall be securely in accordance with the **Section 4.24** "**Information Exchange**".
4. Same Security measures shall be taken on Backup data as of production live data.

4.10 DATA RETENTION

1. All data/Information including Cardholders' shall be retained as per Bank's policies, regulatory requirements and statutory requirements .

4.11 EQUIPMENT SECURITY

1. Equipment shall be placed in secured and controlled areas to minimize unnecessary or unauthorized access.
2. Equipment requiring special protection shall be isolated from other systems and special treatment shall be executed to minimize associated risks.
3. All IT equipment shall be prominently securely marked by branding/tagging or etching.
4. Equipment shall be disposed-off as per **Section 4.30** "**Disposal of Stored Data/Information**"**.**

4.12 INTERNAL TRAINING/TEST INFORMATION SECURITY LAB SECURITY

1. The production environment shall be at least logically segregated from training or test labs /environments where possible and financially viable.
2. The traffic between production and lab/test environment shall be restricted.

4.13 PHYSICAL AND ENVIRONMENTAL SECURITY

1. Access to sensitive data processing areas shall be controlled and monitored.
2. Access to all information processing facilities and secure areas shall be secured through controlled mechanism.
3. Access to Bank's IT Asset shall be protected from unauthorized access.
4. Hazardous or combustible materials shall not be stored in information processing facility(ies)/Data Centers.
5. Back shall have comprehensive Disaster Recovery arrangements and provisions to continue the business in the event of disaster.
6. Bank shall develop a comprehensive enterprise level BCP and DR plan including annual drill and monitoring mechanisms.
7. Bank shall share the drills results with senior management and Board.
8. Back-up media and disaster recovery site (DRS) shall be sited at a geographically/physically separated from primary site.

9. Appropriate firefighting equipment shall be suitably placed to be used in hazardous conditions. This equipment shall be maintained by respective function as per vendor specifications and the Bank’s internal requirements.
10. All employees of the Bank shall use identification badges/access cards in a way so that it shall be clearly visible.
11. Lost or stolen identity badges/card must be reported to issuing authority on priority basis.
12. All personnel are responsible for immediately informing his/her line manager in case of unauthorized access to Bank's resources.
13. Cameras/CCTV shall be installed in sensitive areas for monitoring of activities and recording of camera shall be reviewed for anomalies.
14. For cardholder data processing area, security camera’s recording shall be retained for minimum of three months or as per regulatory requirement. These video logs shall be reviewed periodically or as per business requirement.
15. Inventory of all IT Assets shall be maintained by ITG with necessary asset details including but not limited to asset owner, make, model of device, MAC address, location of device, serial number.
16. All devices especially POS/ATMs, placed in sensitive areas shall be periodically checked and reviewed for swapped/dipped or fraudulent replacement, device tempering etc. by the concerned staff.
17. Offsite Information Assets shall be secured with appropriate controls and security measures.
18. Sensitive data processing areas shall be equipped with redundant power sources to protect unplanned shutdown.

4.14 NETWORK & SYSTEMS SECURITY

1. Security controls shall be established to safeguard the confidentiality, integrity and availability of information passing over networks to protect the connected systems and applications as per business requirements.
2. Appropriate logging and monitoring of the systems and networks shall be enabled and applied in order to trace the activities. All changes shall adhere to Network Security and User Procedure.
3. Audit logs recording user activities, exceptions, and information security events shall be produced and kept as per regulatory and statutory requirements.
4. Assets list of Systems and Network devices shall be maintained and updated periodically especially but not limited to PCI-DSS in scope devices.
5. Access to Web based interfaces especially for administrative access shall be encrypted.

4.14.1 NETWORK SECURITY

1. Firewalls shall be installed, monitored, and maintained at each internet connection, demilitarized zone, internal Bank network and cardholder data environment to serve its objectives.
2. A network diagram detailing all the inbound and outbound connections especially to equipment related with CDE shall be maintained and reviewed at least every six (06) months or as per regulatory requirement.

3. Network devices (including firewalls and routers) configuration and their details shall be documented and maintained which includes but not limited to list of services, protocols and ports along with business justification. Their backup shall be taken as per "**Data Backup Security**" **Section 4.9**.
4. All inbound network traffic shall be blocked by default, unless explicitly allowed and the business justification shall be documented and shall be periodically reviewed by concerned teams.
5. All outbound traffic has to be authorized by management (i.e. what are the white listed category of sites that can be visited by the employees) and business justification shall be documented and shall be periodically reviewed by concerned teams.
6. Network devices configuration shall be reviewed at least on a six (06) months basis to validate its justification. [PCI DSS v3.2, Clause 1.1.7]
7. Only Bank's designated central time server shall receive time signals from external source that shall be based on International atomic time or UTC.
8. All systems shall receive time only from designated central time server and only authorized personnel shall have access to change/update time data with genuine business need.
9. All systems shall have correct and consistent date and time.
10. Any changes to time synchronization settings shall be logged.
11. CDE shall be at least logically segregated from other environment.

4.14.2 SYSTEM SECURITY

1. Baseline configurations for hardening shall be developed under industry best practices.
2. All new and existing systems shall be hardened as per baseline configurations.
3. All default accounts and passwords for the systems shall be changed or disabled at the time of provisioning the system.
4. Any insecure protocols, daemons, services in use shall be documented and justified and approved from management.
5. All unnecessary functionalities like scripts, drivers, etc. shall be removed from systems.
6. System services and parameters shall be configured to prevent the use of insecure technologies like telnet and other insecure remote login commands.
7. Only one primary function per server for CDE shall be implemented to prevent functions that require different security levels from co-existing on the same server.
8. For CDE and other critical systems, change-detection mechanism shall be deployed (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and comparison of critical files shall be performed at least weekly and any discrepancy if found shall be reported to relevant stakeholder for further investigation and remediation.
9. Shared hosting providers must protect each entity's hosted environment and cardholder data.

4.15 WIRELESS COMMUNICATION

1. All wireless Access Points/Base Stations connected to the corporate network shall be installed with the consent of IT Operations.

2. All wireless network access points and controllers shall be secured to mitigate unauthorized access.
3. Implementations shall support a hardware address that can be registered and tracked, i.e., a MAC address.
4. The SSID shall be configured in such a way that it does not contain any identifying information of Bank, such as the Bank's name, group/functional title, employee name.
5. All wireless networks, gateways and handheld devices shall be protected, controlled, monitored and restricted for unauthorized use.
6. Bi-annually scanning shall be performed to discover any unauthorized/rouge wireless access points connected to Bank's network.
7. The firmware on the wireless devices including controllers shall be updated accordingly as per vendors' release schedule, recommendation and Bank's requirements.

4.16 VULNERABILITY MANAGEMENT

1. Bank shall conduct periodic Vulnerability Assessment of Information Assets at least once in a year.
2. Bank shall have a Risk rating/ranking mechanism.
3. All the vulnerabilities shall be assigned a risk ranking.
4. High Risk vulnerabilities shall be on top priority for mitigation/fixation by respective control implementation team and InfoSec Team shall verify the fixation.
5. Bank shall have clear procedure for the implementation of controls.
6. Bank shall perform internal vulnerability scans as and when required but at least once a year for critical information systems and at least quarterly for CDE or after any significant change in the Infrastructure and Application. [PCI 3.2 11.2]
7. For Cardholder data environment, quarterly external network vulnerability scans shall be performed by an Approved Scanning Vendor (ASV) qualified by PCI DSS. [PCI 3.2 11.2]
8. Vulnerability assessment shall be performed at least annually or after any change in application or its infrastructure for all public faced website/web applications. [PCI-DSS v3.2, clause 6.6]
9. Bank shall validate the effectiveness of its information security environment after the vulnerability assessment and fixation. (ETG&RMF 2.7 (a))

4.17 PENETRATION TESTING

1. Bank shall arrange 3rd party penetration testing at least twice in a year or upon any significant change in infrastructure.
2. Internal penetration testing shall be performed bi-annually, upon new deployment, or in case any major changes in infrastructure/application/servers/databases etc.
3. For CDE, Penetration scope shall include CDE perimeter and critical systems including application layer and network layer.
4. If segmentation is used to isolate the CDE from other networks, penetration testing shall be performed at least annually and/or after any significant changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.

5. All vulnerabilities found during penetration testing shall be managed as per Vulnerability Assessment and Penetration Testing procedure.
6. Penetration testing results and remediation activities results shall be retained for at least 01 year.
7. Penetration Result's report shall also be shared with Business Owner.
8. Business Owner(s) shall also ensure the timely remediation of identified vulnerabilities in Penetration Testing results, through ITG.

4.18 IT ASSETS/SYSTEM ACQUISITION

1. Bank shall develop Technology procurement policy in line with regulatory requirements. (ETG&RMF 4.2.2 (a))
2. Policy shall cover the formulation of RFP (Request for Proposal) based upon BRD (Business Requirement Document) including the roles and responsibilities of stakeholders including the approval matrix. (ETG&RMF 4.2.2 (a))
3. Technology procurement process shall be governed and monitor by IT Steering Committee. (ETG&RMF 4.2.2 (h), (i))

4.19 RELEASE MANAGEMENT

Release Management is the process of managing, planning, scheduling, and controlling a software build through difference stages and environments: through testing and deploying software release especially in production environment.

1. All associated updates and corrections to Software, Application, and data shall be documented and shall be duly approved by relevant stakeholders including the business owner.
2. All releases including patches, scripts, and updates shall travel/move from one function to another function with its MD5 (Hash) in order to ensure and maintain the integrity of release.
3. All release packages prior to implementation in production environment shall be tested where possible in test environment and signed off by respective function stakeholders.

4.20 CHANGE MANAGEMENT

1. Any change in systems/ infrastructure shall have a clear business case duly approved & authorized.
2. Based upon business case, relevant stakeholders shall conduct risk & impact analysis of proposed changes and shall be thoroughly tested in test environment before going live in production environment.
3. All change requests shall be logged whether approved or rejected on a standardized repository. The approval of all change requests and the results thereof shall be documented.
4. No single person shall be allowed to effect changes in production systems without the prior approval from appropriate Internal stakeholders; and relevant External stakeholders where applicable
5. Technical Risk Assessment shall be performed for all significant changes in Applications or in the IT Infrastructure.
6. ITG shall facilitate and ensure performance testing of all newly developed critical systems to ensure effective and smooth operation before deploying the same in production environment.

7. Changes shall be tested in an isolated and controlled environment (whether temporary or permanent test environment, if feasible) prior to implementation in production environment.
8. UAT environment shall be logically isolated from production environment.
9. Adequate test scenarios shall be formulated before conducting the test.
10. Changes shall be notified to all stakeholders.
11. File integrity of at least CDE shall be maintained and monitored on weekly basis.
12. Procedures for aborting and recovering from unsuccessful changes shall be documented.
13. Fallback procedures shall be in place to ensure systems can revert back to what they were prior to implementation of changes.
14. System development personnel shall be prohibited from having access to production systems.
15. After completion of significant changes, the security requirements shall be re-assessed and cross checked for respective Information asset.
16. All infrastructure device configurations shall adhere to Bank's standards before being placed on the network and their configurations shall be reviewed annually to maintain its consistency with security requirements of the Bank.
17. Post implementation review shall be conducted at the end of a change to validate the operational performance and deficiencies shall be reported to senior management.

4.21 SOFTWARE INSTALLATION & IPR (INTELLECTUAL PROPERTY RIGHTS)

4.21.1 CONSIDERATIONS FOR SOFTWARE INSTALLATIONS

1. Installation rights shall be restricted to authorized personnel and strictly monitored.
2. All Infrastructure related installations shall be tested in an isolated environment before rolling out in production environment or installing on computing devices.
3. Beta version of software shall not be installed in production servers.

4.21.2 CONSIDERATIONS FOR INTELLECTUAL PROPERTY RIGHTS

1. ITG shall keep the original software, manuals, and backup media except end-user software.
2. Outsourced software development shall be supervised and monitored to protect intellectual property rights, by following the below listed requirements:
   a) Licensing arrangements, code ownership and intellectual property rights protection
   b) Escrow agreement(s) shall be arranged, where feasible

4.22 PERSONNEL SECURITY

1. All Bank employees, contractors, consultants, temporaries, and other workers involved while conducting Bank's business shall be provided information about their obligations pertaining to organization related information security at the time of their induction.
2. All the inductees shall agree and sign the terms and conditions of the employment and their responsibilities for information security.

3. All the inductees shall sign confidentiality and non-disclosure agreement as part of initial conditions of employment.
4. All the employees shall follow Bank Policies during their employment.
5. All personnel of Bank shall be given the awareness on the importance of information security.
6. Incidents affecting security shall be reported through line management to Information Security Group as quickly as possible.
7. Disciplinary actions may be taken on deliberate non-conformity of Information Security policy.
8. All the access rights of employees (permanent / contractual), consultants, temporaries, and other workers including all personnel affiliated with external parties shall be removed and all official assets in possession shall be returned back upon termination/separation of their employment, contract or agreement or adjusted upon change in responsibilities.

4.23 INFORMATION CLASSIFICATION AND CONTROL

1. All information and applications must have documented business owner.
2. Data/information shall be labeled according to its value, sensitivity and criticality and shall reflect its classification level.
3. All data stored, processed and accessed on Bank's information systems (in print or digital format) must be assigned a classification level by the owner or creator/custodian on behalf of owner.
4. All Bank's information shall be categorized into the following classification levels:
   a) **Secret:** Secret data is the most sensitive information and requires the highest level of protection. Such information/data if lost or exposed to outside Bank/publicly available may cause "exceptionally grave damage" to the Bank. Access to Secret information shall be allowed solely to officials with a specific need to know
   b) **Confidential:** Confidential information is the information that Groups/functions may decide to share with other units outside their administrative control within Bank for the purpose of collaboration and collective decision making etc. Such information/data may cause "damage" to Bank if made publicly available
   c) **Internal Use:** Internal operational information which is only shared within Bank, with employees and approved non-employees, and contractors
   d) **Unrestricted (Public):** Bank's information which is suitable for public dissemination falls under this classification, such as Information available on Bank's Corporate Website
5. All secret/confidential information/data shall be protected via access controls.
6. The designated staff of the respective functions/groups shall maintain a list of documents / data / information appropriately classified.
7. By default, all un-classified information will be treated as "Internal Use".

4.24 INFORMATION EXCHANGE

1. Secret and confidential classified information while in transit outside the Bank's network shall be encrypted or well protected to ensure the confidentiality, integrity and authenticity of information.

2. Bank has a legitimate right to capture and inspect any data stored on or transmitted over its Information System Facilities (regardless of data ownership).
3. All media types shall be classified as per **Section 4.23 "Information Classification and Control"**.
4. Internal or External distribution of all kind of media shall be strictly controlled.
5. Media movement shall be via secured courier or any other secure delivery method that can accurately be trackable.
6. Movement of media especially but not limited to media of secured area shall be approved from management prior to movement.

4.25 INFORMATION RISK MANAGEMENT

1. Information Security Group shall identify and classify technology risks and respective stakeholders shall implement risk mitigation as appropriate.
2. Technical Risk Assessment shall be performed as per regulatory requirement for Applications and Infrastructure before the deployment in the production environment and when there is a significant change in the Application or its Infrastructure.
3. Respective functions shall provide information necessary to perform information risk assessment within due time.
4. Business owner shall expedite and ensure that actions have been taken immediately to mitigate the identified risk(s).
5. Bank shall evaluate the risk processes in place through testing methodologies and risk review of controls. The result of these exercises shall be duly reviewed by the management and major risks shall be reported to IT steering committee.

4.26 INFORMATION RISK ACCEPTANCE AND DISPENSATION

1. The risks to Bank's information, data, systems, and networks shall be reduced to minimize the impact of threats and vulnerabilities.
2. Each function can accept a risk due to technical, cost, or other reasons, prudent for business operations. However, any function accepting a risk will be responsible for its decision.
3. In case the non-compliance with Information Security Policy results in harm to Bank's information, data, systems or networks the non-compliant function shall be responsible.

4.27 INFORMATION SECURITY POLICY FOR OUTSOURCING

On business need basis Bank may utilize IT outsourcing services within Pakistan and abroad, within the parameters of Bank outsourcing policy and SBP provided guidelines (*Ref SBP Circular: BPRD Circular No. 06 of 2017 Framework for Risk Management in Outsourcing Arrangements by Financial Institutions*).

1. Bank shall internally carry out due diligence of the business activities to be outsourced.
2. Bank's NDA shall be signed with external parties by respective function prior to exchanging confidential information or formal agreements.
3. Bank shall carry out detailed due diligence for the intended service provider(s) and shall document the same for further reference and record.

4. Provision in the agreement shall be made in favor of the regulator (SBP) for any inspection of outsourced functions including inspection of all related documentation at any time.
5. In any outsourcing arrangement, the accountability for the business activity remains with the Bank's concerned Team.
6. All Groups/functions shall ensure that the requirements of security and contingency planning shall be met as per Bank's policy & SBP Guidelines.
7. Bank shall review the service provider at least on an annual basis to ascertain its ability to deliver the outsourced services in the manner agreed as per SLA.
8. All outsourcing service providers must be regulated by their respective regulator of the country.
9. Outsourcing arrangement of all IT equipment and IT services shall be approved by ITSC.
10. IT outsourcing shall not be allowed for critical IT systems /functions and applications of the Bank like core banking applications including Branchless Banking, mobile wallets of Branchless Banking, Main database, databases relating to information of customers, information security and Primary & Disaster Recovery Sites.
11. Bank shall execute Software Escrow Contracts for critical customized software with the software developer or service provider.

4.28 INFORMATION SECURITY POLICY FOR IN-SOURCING

1. Bank shall consider all in-sourcing personnel as 3rd party and all applicable regulatory and the bank's Information Security policy clauses pertaining to 3rd party shall be applied.

4.29 CYBER SECURITY CONTROLS

1. Banks shall strictly implement Information Security Control to safeguard bank's information assets from cyber threats and attacks.
2. Bank shall develop cyber security action plan to proactively address the likely cyber-attacks in order to anticipate, withstand, detect, and respond to cyber-attacks in line with international standards and best practices. (ETG&RMF 2.1 (d), ETG&RMF 2.5)
3. Bank shall Implement automated solutions to monitor and proactively track cyber-attacks. (ETG&RMF 2.5 (e))

4.30 DISPOSAL OF STORED DATA/INFORMATION

1. Appropriate disposal mechanism shall be in place for destruction of sensitive information in both paper and electronic media.
2. All electronically data shall be securely disposed-off by ITG when no longer required by Bank, regardless of the media or application type on which it is stored. *[BPRD Circular no. 5 2017, Enterprise Technology Governance and Risk Management Framework, Clause 2.4.1]*
3. A process shall be in place to identify and dispose off all data exceeding retention period while a quarterly process for cardholders' data shall be followed. [PCI DSS v3.2 3.1]

4.31 LOG REVIEW

1. Bank shall maintain appropriate logs of applications, system, networks, and databases especially to ensure the traceability of transactions and related events and shall retain for a period as defined by regulatory authorities.
2. Log data shall at least capture the following data elements, where possible:
   - User identification
   - Type of event
   - Date and time
   - Success or failure indication
   - Origination of event
   - Identity or name of affected data, system component, or resource
3. Log data review shall at least cover the following:
   - All actions taken by any individual with root or administrative privileges
   - All invalid logical access attempts (failed logins)
   - Any use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges
4. Logs review of CDE shall be automated and reviewed as per PCI DSS requirements.
5. Exceptions and anomalies identified during the review process shall be discussed and reviewed with concerned group on regular basis.
6. Log files shall be protected from modifications and their access to shall be controlled and monitored.
7. Bank shall review alerts generated by file integrity software to detect any modification in log files.
8. Logs/Alerts shall be continuously monitored for all security control systems especially but not limited to critical security systems like IPS, IDS, Firewalls, FIM etc.

4.32 SECURE APPLICATION DEVELOPMENT

1. Bank shall ensure that application development adhere the secure coding practices and at least mitigating top 10 vulnerabilities mentioned by OWASP.
2. Bank shall have Software Quality Assurance mechanism in place for all business applications which shall be independent of Software development function and administration.
3. Only validated code shall be implemented into Bank's production environment, which shall be recommended by Bank's Software Quality Assurance, after necessary approvals.

4.33 SECURITY INCIDENT MANAGEMENT

1. Bank shall monitor and record/document security breach incidents and report the same to BoD, senior management, and to the regulator as per regulatory requirement on prescribed reporting template attached as **Annex C.** (ETG&RMF 2.6 a, b)
2. It is the responsibility of all employees to report Security Incidents to their line management, ITG, and InfoSec as soon as they know about the incident. Employee will not communicate the same with external

bodies including law enforcement agencies and public without prior authorization of senior management.

3. Security Incident Response plan shall be in place to manage incidents related with Information Security.
4. Banks shall have Incident Response Team having sufficient knowledge & experience of their respective function.
5. Bank shall conduct root cause analysis by engaging all relevant stakeholders and shall conclude the analysis with proper mitigation plan.

4.34 ENCRYPTION

1. Bank shall secure sensitive data at-rest, in-motion and data in-use shall be masked, where necessary.
2. Encryption keys and key-generating solution (equipment, application, software) shall be managed securely by Bank and keys shall be stored securely in fewest possible locations. [PCI DSS V3.2 3.5.4]
3. Dual Control shall be implemented for encryption key management.
4. Keys for key encrypting shall be different from data encryption keys. [PCI DSS V3.2 3.6.6]
5. Encryption keys shall be changed after the defined cryptoperiod. [PCI DSS V3.2 3.6.4]
6. Key custodian shall have to formally acknowledge his responsibilities as encryption key custodian along with his responsibilities.
7. Strong encryption shall be used for all privileged access to databases, systems, and networks, where possible.
8. To ensure validity and correctness of encryption, encryption process shall be validated at least annually.
9. Encryption shall be used for all wireless (Wi-Fi) services available within Bank premises.
10. Key-generating solution (equipment, application, software) shall be physically and logically secured.
11. Retirement or replacement of keys shall be done as deemed necessary or keys are suspected of being compromised. [PCI DSS V3.2 3.6.5]
12. Encryption keys substitution shall be controlled to prevent unauthorized substitutions.

4.35 INFORMATION/CYBER SECURITY AWARENESS AND TRAINING

1. Bank shall arrange adequate Information/Cyber Security Awareness program for permanent & contractual staff members.
2. Bank shall take necessary measures to disseminate Information/Cyber Security Awareness message for its customers.
3. Bank shall ensure that staff members are provided with trainings, professional courses, and certifications as and when required and will facilitate them to renew their knowledge and credentials on time-to-time basis to ensure effectiveness of the staff members.
4. Bank shall collaborate with industry for the purpose of collecting and exchanging timely information that may facilitate in detection, response, resumption and recovery of systems. (ETG&RMF 2.9 (a), (c), (d), (e))
5. Secure coding training/sessions shall be imparted for application developers at least annually and upon joining.
6. Bank shall clearly display on information system (where necessary) that:

a) Any information stored, transmitted or handled by these systems is the property of Bank These systems may be monitored for administrative, security and other lawful purposes

4.36 COMPLIANCE WITH LEGAL REGULATORY & CONTRACTUAL REQUIREMENTS

1. InfoSec Policy has been devised to cover statutory and regulatory requirements including the contractual obligations, however due to any reason if Information Security Policy contradicts with the above mentioned requirements then statutory and regulatory requirement will prevail.

4.37 DATA LEAK PREVENTION

1. Bank's staff shall maintain the confidentiality according to the classification of the information.
2. Adequate measures shall be taken to restrict unauthorized transfer of classified information.

4.38 DATA LOSS PREVENTION

1. Bank shall take necessary measures to prevent data losses.
2. Appropriate solution(s) shall be deployed to maintain backups as per business need and regulatory requirements to prevent the data loss.

4.39 BUSINESS CONTINUITY AND DISASTER RECOVERY

1. Bank shall develop a comprehensive Business continuity and Disaster Recovery Plan.
2. BCP shall be drafted to minimize financial losses, serve customers with minimal disruptions and mitigate the negative effects of disruptions on business operations.
3. Bank shall also develop a comprehensive diester Recovery Plan.
4. DR Plan shall be drafted to minimize the recovery time of the site, equipment, and infrastructure.
5. Plan shall be tested and validated at least annually.

5 Annexures

5.1 Annexure A - Risk Acceptance by Clause(s) Exception Form

This form shall be submitted in advance at-least 03 working days of the expected start date of the exception period.

Section A: Requestor Information

Name of Employee:	EIN:
Functional Title:	Email:
Phone:	Location:

Details of Requested Policy Exception/Justification

In the space below, please detail the circumstance(s) that shall require the exception and the business reason(s) for the exception. Please attach additional pages if needed.

From _____________ To ____________

Details:

a. Policy Clause reference: ____

b. System/Network/Application detail: ____

c. Other details:

Unit Head **Divisional Head**

Section B: Associated Risk(s)

In the space below, please detail the associated risk(s) for the acceptance by the relevant Group.

*To be filled by InfoSec

We hereby accept the above-mentioned risk(s) associated with the exception.

Group Head (Concerned) **Group Chief (concerned)** **Group Chief (ITG)**

Recommended by:

Group Head (InfoSec) **Group Chief (RMG)**

Approved by:

CEO

5.2 Annexure B

Compliance Group Responsibilities for Technical Compliance:

1. Review of Information Security Policies & Procedures to ensure their compliance with Regulatory guidelines and report non-conformities.
2. Ensure compliance regarding all Information System Inspections /Audit observations reported by internal/ external/ regulatory auditors.
3. Follow-up compliance of issues identified in the Information Security Assessments with ITG and ensures timely mitigation.

5.3 Annexure C

Details of Established Security Breaches

For the Quarter Ending: ________________

Sr.	Source of security breach discovery	Nature of security breach	Reasons for the occurrence of security breach (e.g. Breach of control, Procedures were not followed, weakness in implemented security controls etc.)	Impact of security breach (e.g. on bank business, systems, customers etc.)	Action(s) taken to rectify the Security Breaches	Remarks (further details, if any)

6 REVISION HISTORY

Revision Number	Updated by	Short Description of Revisions	Date
Version 1.0		First draft of information security policy, presented to BoD for approval.	October 10, 2007
Version 2.0		Information Security Policy was revised according to ISO 27001:2005 guidelines.	August 23, 2010
Version 3.0		RMG and ITG have jointly endeavored to rationalize the number of documents by amalgamating the 25 independent documents into one coherent policy document, while simultaneously ensuring that the policy requirements are in sync with the present IT infrastructure of the Bank.	April 25, 2014
Version 4.0		Full review of InfoSec Policy w.r.t Enterprise Technology Governance and Risk Management Framework and PCI-DSS v3.2	

7 DEFINITIONS & ACRONYMS

Following definitions and acronyms have been used in this document.

7.1 DEFINITIONS

Access Control: Access control (AC) is the selective restriction of access to a place or other resource(s) based upon Information Security and Business requirements.

Accountability: Responsibility of an entity/individual for its actions and decisions.

All functions: All relevant groups.

Asset: Anything that has value to the organization.

Asset Custodian/Administrator: Asset custodian/administrators are individuals or entity responsible for administering assets.

Asset Owner: Asset Owners are individuals or entity who have the ownership of assets. *Asset Owner and Information Asset Owner are interchangeably used in this document.*

Authenticity: Authenticity is the quality of being genuine or real.

Authorized Devices: Devices which has been approved and allowed by the Bank.

Availability: Property of being accessible and usable upon demand by an authorized entity.

Bank: The Bank referred to Allied Bank Ltd.

Cipher: A cipher is a method of hiding words or text by applying different techniques for replacing original letters with other letters, numbers and symbols.

Cardholder Data: At a minimum, cardholder data consists of the full PAN (Primary Account Number). Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code

Critical systems: All systems which must be up and running within 04 hours after disruption.

Confidentiality: Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Control: Control is used as a synonym for safeguard or countermeasure.

Corrective Action: A corrective action is action to address nonconformity that has occurred.

Cryptography: Cryptography is associated with the process of converting ordinary plain text into unintelligible text and vice-versa.

Cryptoperiod: A cryptoperiod is the time span during which a particular cryptographic key can be used for its defined purpose.

Cyberspace: The interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.

Cyberattack: A cyberattack is any type of offensive maneuver employed by nation-states, individuals, groups, society or organizations that targets computer information systems, infrastructures, computer networks, and/or personal computer devices by various means of malicious acts usually originating from an anonymous source that either steals, alters, or destroys a specified target by hacking into a susceptible system.

Cybersecurity: Cybersecurity is a subset of information security and the practice of defending organization's networks, computers and data from unauthorized digital access, attack or damage by implementing various controls in shape of processes, technologies and practices.

Data: Data are plain facts. The word "data" is plural for "datum." Data is the raw material that can be processed by any computing machine. Data can be represented in the form of numbers, images, sounds, multimedia, animations and words. Data is collected through a mechanism which provide assurance of the origin and integrity of a message.

Data Leakage: The unauthorized transfer of classified information from a computer or datacenter to the unauthorized person/entity(s). Data leakage can be accomplished by simply mentally remembering what was seen, by physical removal of tapes, disks and reports or by subtle means such as data hiding.

Data Loss: Data loss is an error condition in information systems in which information is destroyed by failures or neglect in storage, transmission, or processing.

Data at Rest: Data that is stored on storage.

Data in Transit: Data that is traversing over the network or systems.

Data in Use: Data that is in use or processed by user and/or system according to business needs.

Demilitarized Zone: A network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's policies for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks.

Due diligence for Outsourcing: Due diligence process of service provider shall encompass assessment of all areas including its experience, technical competence, financial strength, reputation, existence of control framework, performance standards, managerial skills, policies & procedures, reporting &monitoring environment and business continuity planning. The due diligence shall also address other issues, such as potential conflicts of interest in case service provider is related/affiliated party, or where it provides similar services to competitors. In case of the single service provider enhanced due diligence shall be conducted to identify and mitigate new risks. The FI's shall also identify all potential and actual conflicts in the FI are outsourcing operations to ensure that the conflicts are identified and avoided or prudently managed.

Efficiency: Efficiency signifies a level of performance that describes a relational process that uses the lowest or same amount of inputs to get the better amount of outputs.

Encryption: Process of ciphering the messages (or information) in such a way that unauthorized parties cannot read it, but only authorized parties can.

Equipment: IT equipment used in Bank unless explicitly mentioned.

Event: Anything that happens or takes place such as user actions, system occurrences of a particular set of circumstances.

External Stakeholder: A person/function/entity belong to third-party with an interest or concern in something, especially a business

Framework: A set of related policies and procedures.

Guideline: Recommendation of what is expected to be done to achieve an objective.

Impact: Tangible and/or intangible effects (consequences) of one thing's or entity's action upon business objectives.

Incident: Incident is an undesired event where business disruption reaches beyond the tolerance level of the organization. Any event that is either unpleasant or unusual.

Information: Information is data that has been processed in such a way as to be meaningful to the person who receives it. it is anything that is communicated.

Information Asset: Knowledge or data that has value to the organization.

Information Security: Safe-guarding an organization's data from unauthorized access or modification to ensure its availability, confidentiality, and integrity.

Information Security Event: A security event is any observable occurrence that is relevant to information security and may potentially have information security implications.

Information Security Incident: A security incident is a security event that resulted in damage or risk to information security assets and operations.

Information Security Management System (ISMS): An information security management system (ISMS) is a set of all of the policies, procedures, documents, records, plans, guidelines, agreements, contracts, processes, practices, methods, activities, roles, responsibilities, relationships, tools, techniques, technologies, resources, and structures for systematically managing, controlling and preserving an organization's sensitive data and information. The goal of an ISMS is to minimize risk and ensure business continuity by pro-actively limiting the impact of a security breach.

Information Security Risk: Potential that a threat will exploit a vulnerability of an asset or group of assets and thereby cause harm to the organization.

In-sourcing: A business in which work that would otherwise have been contracted out is performed in-house. For example, an IT outsourcing provider may be hired to service a company's IT department while working inside the company's facilities. In addition to contracting an entire team of workers from an outsourcing provider, outside experts are sometimes hired as consultants (to improve certain processes etc.) and the internal staff thereafter implements their recommendations.

Integrity: Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle.

IT Equipment: Information Technology devices used in the processing, storing, transmitting the data electronically. The following are some examples of IT equipment:

1. Servers, personal computer, laptops, tablets, smart phones and all peripheral units associated with such computers.

2. Routers, switches, local area networks, private branch exchanges, network control equipment, or microwave or satellite communications systems.
3. Magnetic tape units, mass storage devices, printers, video display units, data entry devices, plotters, scanners, or any device used as a terminal to a computer and control units for these devices.

Jail Broken or rooted device: Jailbreaking refers to the process of removing all restrictions imposed on an iOS device. Rooting is a process that allows you to attain root access to the Android operating system code. These give the privileges to modify the software code on the device or install other software that the manufacturer wouldn't normally allow.

Licensed Software: Permission to use a software on non-exclusive basis, and subject to the listed conditions. A software license does not automatically transfer the ownership of the software.

Locking the Computer: It is a process similar to logging-out but keeping everything open and running as-is so that all activities continue in background without closing program and services running on the computer. To unlock the computer, authentication is required.

Mobile Devices: Mobile Devices Includes Tablets, Cell Phones, iPad etc. excluding laptops and Personal Computers.

MD5: The MD5 algorithm is a widely used hash function producing a 128-bit hash value. It is widely used for verifying the integrity of a computer file.

Outsourcing: Use of a third party (affiliated entity or un-affiliated) to perform activities, functions or processes normally to save money, time and/or use the skills/technology of another

entity on a continuing basis that would normally be under taken by the Bank, now or in the future. However, it will not cover consultancy services, purchase contracts for tangible/intangible items, for example, contracts to purchase standardized products such as furniture, Software/IT solutions, Automated Teller Machines (ATM) etc.

Penetration Testing: Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit. There are broadly three methods:

1. **White-box testing:** White-box testing (also known as clear box testing, glass box testing, transparent box testing, and structural testing) is a method of testing software that tests internal structures or workings of an application, as opposed to its functionality. In white-box testing an internal perspective of the system, as well as programming skills, are used to design test cases..
2. **Grey-box testing:** Grey Box testing is testing technique performed with limited information about the internal functionality of the system which includes but not limited network, software and infrastructure etc.
3. **Black-box testing:** Blackbox penetration test requires no prior information about the target network or application and is actually performed keeping it as a real-world hacker attack scenario.

Policy: Overall intention and direction as formally expressed by management.

Power User IDs: Power user IDs (like Administrator IDs, Root User IDs, privileged User IDs etc.) are computer users' IDs which used for management, monitoring and reporting of advanced features of computer hardware, operating systems, programs, or websites which are not used by the average/normal user IDs.

Preventive Action: Action to eliminate the cause of a potential non-conformity or other undesirable potential situation.

Procedure: Specified way to carry out an activity or a process.

Process: Set of interrelated activities that interact with one another and use resources to transform inputs into outputs.

Production Environment: Production environment is a term used mostly by developers to describe the setting where software and other products are actually put into operation for their intended uses by end users.

Pyramid Schemes: A pyramid scheme (commonly known as pyramid scams) is a business model that recruits members via a promise of payments or services for enrolling others into the scheme.

Record: Document stating results achieved or providing evidence of activities performed.

Risk: The potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability.

Risk Acceptance: Decision to accept a risk by the management of the Bank.

Risk Analysis: Systematic use of information for identifying and quantifying uncertainties, estimating their impact on outcomes.

Risk Assessment: Overall process of risk analysis and risk identification.

Risk Management: Coordinated activities to direct and control an organization with regard to risk or uncertainty which influence in achieving the objective.

Risk Mitigation: Process of selection and implementation of measures to bring risk at minimum/acceptable level.

Rouge Wireless Access Point: Rogue wireless access point is an access point that has been installed on a secure network without explicit authorization from a local network administrator, whether added by a well-meaning employee or by a malicious attacker.

Sensitive Area: "Sensitive areas" refers to any datacenter, server room or any area that houses systems that store, process, or transmit sensitive data.

Sensitive Data: Data that is protected against unwarranted disclosure.

Sensitive Information: Information that is protected against unwarranted disclosure.

Service Code: Three-digit or four-digit value in the magnetic-stripe that follows the expiration date of the payment card on the track data.

Simple Network Management Protocol (SNMP): An Internet-standard protocol for managing devices on IP networks.

Stakeholder: A person/function/entity with an interest or concern in something, especially a business.

Statutory Requirement: Statutory requirements are those requirements which are applicable by virtue of law enacted by the government.

Threat: Any potential occurrence, if realized, may cause an undesirable or unwanted outcome for an organization or for a specific asset.

Unrestricted External Access: Access to network from outside by using the unmanaged ports which are used during session handshake.

Vulnerability: Weakness of an asset or control that has potential to be exploited by a threat.

Vulnerability Scanning: The automated process of proactively identifying security vulnerabilities in computing systems or in a network in order to determine if and where system can be exploited and/or threatened.

Workstations: Workstations includes Personal Computers and Laptops//.

7.2 ACRONYMS

ABL	Allied Bank Limited
ATM	Automated Teller Machine
B2B	Business to Business
B2C	Business to Customer
BoD	Board of Directors
CDE	Cardholder Data Environment
CG	Compliance Group
CHD	Cardholder Data
CRO	Chief Risk Officer
DH	Divisional Head
DRS	Disaster Recovery Site
ETG&RMF	Enterprise Technology Governance & Risk Management Framework for Financial Institutions, issued vide BPRD Circular No. 05 dated May 30, 2017
FIM	File Integrity Monitoring
GC	Group Chief
GH	Group Head
HRG	Human Resource Group
ICT	Information Communication Technology
IDS	Intrusion Detection System
InfoSec	Information Security
IPS	Intrusion Prevention System
IT	Information Technology
ITG	Information Technology Group
IS	Information System
ISM	Information Security Management
MAC	Media Access Control
NDA	Non-Disclosure Agreement
OWASP	Open Web Application Security Project
PCs	Personal Computers
POS	Point of Sale
PII	Personal identifiable Information

RFP	Request for Proposal
RMG	Risk Management Group
SAD	Sensitive Authentication Data
SIEM	Security Information and Event Management
SBP	State Bank of Pakistan
SNMP	Simple Network Management Protocol
SSID	Service Set Identification
SDLC	Software Development Life Cycle
SQL	Structured Query Language
TRA	Technical Risk Assessment
UAT	User Acceptance Testing
VPN	Virtual Private Network