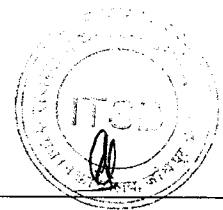# Rajasthan Marudhara Gramin Bank
Information Technology Service Department
Head Office, Jodhpur

Information Security (IS) Policy
Standards and Procedures

आरएमजीबी
R M G B

Version	7.0
Date of Adoption	2 2 OCT 2024
Renewal Frequency	Annually
Last Review Date	22.12.2023

Rajasthan Marudhara Gramin Bank

A. Objective of IT Policy

The objective of the IS Policy is establishing suitable levels of security for Information Systems including but not limited to all Cloud environment commissioned or run by Bank computer, storage mobile devices, network software and data. Confidentiality, Integrity and Availability of the information and mitigating the risk associated with the theft, loss, misuse, damage or abuse of these System also, continuous improvement of any information Security Management System(ISMS) will be undertaken.

This policy also provides the principles by which a safe and secure information system's working environment can be established for Staff, management and any other authorized user. It aims at educating and ensuring that all users understand their own responsibility for protecting the Information System's data which they handle.

B. Document Distribution

This document is owned by BANK (RRB)'s General Manager (In charge-Information Technology Services Department).

C. Primary recipients

All Employees of the Bank

D. Authority

The policy document is issued under the authority of Board of Directors.

E. Standards & Procedures

Standards are detailed requirements that need to be met for complying with the IT Policy & IS policies. Separate set of standards have been developed for each policy statement. Standards include measures that need to be taken for mitigating all risks associated with the respective domain covered by the policy statements. Procedures are detailed guidelines of how to implement the measures and who should be responsible for the implementation.

F. Scope

This policy is applicable and will be communicated to all employees, TSP and other users who interact with information held with bank and information

system used to store and process.

G. Management of IS policy

GM shall review and approve the IS Policy and Standards for further approval of Board of the Bank. GM shall assist ITSD in framing, review of the policy, dissemination and enforcing of approved IS Policy & Standards and related activities in the Bank.

IS Policy & Standards shall be reviewed at least annually by the GM and any amendments to the plan shall be approved by the Board of the Bank. ITSD shall assist CISO in performing his responsibilities towards IT subcommittee and Information Security.

H. Responsibilities

H.1. The IT Sub Committee of RMGB is responsible for approving the standards and procedures and approving any subsequent modifications for achieving desired level of information system security in line with Business Requirements.

H.2. IT Sub Committee is responsible for ensuring that standards and procedures are current and reflect the requirements of the Bank with the help of Information Technology Service Department.

H.3. Controllers/Application Owners/Dept. Heads/Heads of all branches are responsible for implementing and enforcing the relevant portions of the standards and procedures within their jurisdiction.

H.4. ITSD is also responsible for dissemination of the standards and procedures.

H.5. Inspection & Management Audit Dept. is responsible for IS auditing the level of compliance with the standards and procedures.

I. Compliance

The Bank expects all employees and authorized external personnel including vendors to comply with these standards and procedures. Failure by any employee of the Bank to conform to applicable standards & procedures may result in disciplinary action. Vendors shall be dealt with according to the contracted covenant.
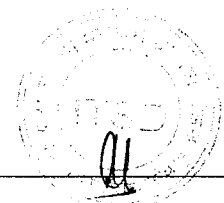
J. Exception

Exceptions or deviations from the policy, standards, procedures & guidelines will be processed as follows:

Approving Authority: CISO
Exception Criteria: The following criteria will be used

    a) Existence of a genuine need for exception
    b) Adequacy of compensating controls

Workflow: Head– IT will assess and submit all requests with his recommendations to the CISO.

Registration & Tracking: All such requests will be registered, tracked and submitted for subsequent review to CISO through IT Head.

Duration, Expiry & Review: All Exceptions or Deviations, when approved, should be for a minimum period and the period should not exceed ONE YEAR in any case in one instance. Any extension requests should be reviewed and assessed again before expiry of the approved period as per the same workflow & criteria mentioned above.

K. Review

ITSD will review this policy and standards and procedures every year, based on user inputs, independent review reports, compliance reports or new risk exposure and propose changes wherever required. ITSD will also review and propose changes to the standards and procedures when significant security breaches / incidents occur in the Bank and based on applicable legal and regulatory requirements.

IS Policy

Table of Contents

1 Application Security

1.1 Policy Statement

1.1.1 Applications deployed in the Bank will have controls for secure input, processing, storage and output of data. Applications must be tested for security and performance before deployment and should be managed for high availability. Access to application must be restricted to authorized persons and rights provided on the principle of least privilege.

Standards and Procedures

1.2 Application Owner

1.2.1 The GM ITSD should be the designated owner for all application deployed within the Bank. It has overall responsibility for application security in all activities including outsourced activities related to design, development, deployment, management and support.

1.2.1.1 GM ITSD should obtain application integrity statements in writing from the application development vendors providing for reasonable level of assurance about the application being free of malware at the time of sale, free of any obvious bugs, and free of any covert channels in the code (of the version of the application being delivered as well as any subsequent versions/modifications done), and free from OWASP vulnerabilities for web applications.

1.3 Application Access

1.3.1 User Access and Password Management Policy should be referred for authentication of user, creation of user ID, assignment of privilege levels, password management, user access review, logging and related user management activities in Applications

1.3.2 Application should display the following information on completion of a successful log-on:

1.3.2.1 Date and time of the previous successful logon.

1.3.2.2 Details of any unsuccessful login attempts since the last successful logon.

1.3.3 This will help the user to easily identify if there has been any unauthorized access (successful/unsuccessful) using his credentials.

1.4 Data Security

1.4.1 Encrypted data communication channels should be setup to ensure that integrity and confidentiality of data is maintained.

1.4.2 No official, assigned with responsibility of administration of application, should have access to edit the database from back-end.

1.4.3 Application should have facility to check the integrity of data.

1.5 Input Controls

1.5.1 All user inputs should be checked by the application to ensure it is both appropriate and expected. The software should have adequate controls to ensure that, data has been accurately input e.g. range checks, validity checks, etc.

1.5.2 Each transaction should be recorded in such a way that it can be established that it has been input to the system. The application should have additional controls to ensure that all recorded transactions are input to the system and accepted only once. Rejected transactions should be reported.

1.5.3 Batch jobs should have following set of guidelines:

1.5.3.1 There should be controls to ensure that all the entries have been uploaded without any omission.

1.5.3.2 There should be a restart facility for batch jobs if they terminate abruptly.

1.5.3.3 The user-id of the person who executes the batch job should be embedded in the transactions.

1.5.3.4 There should be an event log for batch processes.

1.5.3.5 If there are any temporary files created by the batch job, these should be deleted before the end of job.

1.5.3.6 If there are multiple jobs within a batch process that needs to be executed sequentially, there should be controls to ensure that a new job is taken up only after successful completion of the previous one. In case one of the jobs fails, the process should exit without continuing with the remaining jobs.

1.5.4   If two users are accessing the same recordat the same time application should ensure database consistency. To prevent inconsistency and lost updates, record locking needs to be implemented in the database application.

1.6 Processing Controls

1.6.1   The application should ensure that processes cannot be initiated out of sequence. Application should ensure that all tasks associated with a particular process are completed and cannot be manipulated or bypassed.

1.6.2   The application should have built-in checks to ensure that if there are any pre- requisites for executing a particular process, these are met before initiating the same.

1.6.3   If internal processing is halted in middle of any processing due to any error or failure, all the dependent/ related processes should be appropriately handled to ensure consistency and integrity of data.

1.7 Account Policy

1.7.1   User Access and Password Management Policy should be followed for Account Policy.

1.8 Audit Logs

1.8.1   User Access and Password Management Policy should be followed for Audit logs and logging requirements.

1.9 Firewall

1.9.1   All critical multi-user applications should be placed behind a firewall to segregate from internal and external users.

1.9 Documentation

1.10.1 ITSD is responsible for creating the secure configuration document. This should cover all security settings as specified in the application security policy.

1.10.2 ITSD should ensure that detailed documentation is available for the following activities

- Application installation.

- Configuration settings

- Privilege levels and associated staff categories.

- User Procedures

- Backup and recovery procedure.

- Data retention period

1.10.3 All settings mentioned in the secure configuration document should be incorporated in the application documentation.

1.10.4 Adequate backups of all documentation should be maintained. A copy of all application documentation should be kept at disaster recovery site as well for reference.
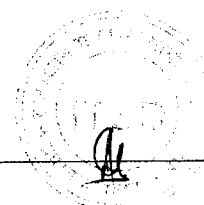
2 Network Security

2.1 Policy Statement

2.1.1 Computer networks of the Bank should be segregated from external networks and all connections to external networks including Internet, outsourced vendors and business partners will be authorized and provided in a secure manner. All remote access to the Bank's network must be authenticated and provided based on business requirements. Network should be designed and maintained for security and high availability to meet the requirements of the users.

Standards and Procedures

2.2 Network Management Responsibility

2.2.1 IT Dept shall have the overall responsibility for Bank's entire network including outsourced activities like WAN setup that comprise the Bank's network.

2.2.2 IT Dept shall issue Guidelines for LAN set up at branches/ offices and connectivity with external entities, Internet, business partners etc. and obtain confirmation from the ROs and the administrative units that Networks set up at branches / offices are complying with the Bank's Network Security Policy.

2.2.3 Any changes on Bank's Network, introduction of new network, connection to external network etc. should be done after consultation and approval from IT- Department.

2.3 Internet Access Limitation

2.3.1 The branches/offices can browse only those internet websites that are whitelisted on proxy servers provided by ASP.

2.3.2 The internet access other than proxy services should only be provided to the standalone system after approval from CISO.

2.4 Segregating Server and User Segments

2.4.1 Critical application servers should be protected by Firewalls. These servers should be accessible only from their respective user segments. The Firewall should restrict user access to essential ports on the

respective servers.

2.5 External Networks

2.5.1 IT Dept should ensure that proper controls are implemented to mitigate the risk before allowing connection of the branch networks with external networks including connections to the customers, ASP and business partners that are outside the management of bank.

2.5.2 External networks should be separated from the Bank's network through access control devices or through dedicated firewalls.

2.5.3 Access control device should restrict access to essential IP-Addresses and ports. Wherever feasible, the resources that are required to communicate or accessed by the external network should be segregated on a separate segment of the Firewall. This will ensure that even if the resource accessed by the external network is compromised the Bank's internal network is secure.

2.5.4 Any access on such resources from external network should be secured by user- id/password over encrypted channel.

2.5.5 An automatic session time-out should be set for remote-access technologies after a specific period of inactivity.

2.5.6 All such access should be removed or disabled as soon as the requirement is over.

2.6 Dial-out Access

2.6.1 For any dial-out access business requirement, permission must be taken from the Controller.

2.6.2 The machines used for dial-out connectivity should be isolated from the rest of the LAN connecting to SB Connect.

2.7 Redundancy

2.7.1 Adequate redundancy should be provided for critical network links to ensure that there is minimum disruption of business.

2.7.2 Redundant link should be checked for normal working and automatic switch over periodically.

2.8 Network Management

2.8.1   Physical & Logical ports, and services, which are not specifically required for business functionality, should be protected by disabling/blocking.

2.8.2   Equipment identification should be enabled on network devices based on sensitivity of applications and data communication.

2.8.3   Routing controls should be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.

2.8.4   Network should be configured securely to not to disclose any internal IP addresses and routing information to unauthorized users.

2.8.5   All remote access on Network/Security devices should be protected using   cryptographic techniques like SSH, VPN, SSL for web-based management.

2.8.6   All the network and security devices should be in time synchronization with a standard time device/server. This standard time device/server should be in sync with time value from Industry accepted standards like internet/GPS. This time data should be protected from any unauthorized modifications.

2.9 Access Controls on Network and Security Devices

2.9.1   Access to Network devices should be controlled by Access Control Lists.

2.9.2   Access to Network/security devices should be provided on need to have basis. Physical and logical access for diagnostic and configuration ports should be controlled.

2.9.3   Users Groups should be created in-line with security roles/privilege level required on network/security devices. E.g. Administrator user group, backup user group.

2.9.4   User-id/password should be created under User groups to provide access to authorized users. Such access may be restricted from intended IP addresses only.

2.9.5   Session time-out should be set on all network/security devices.

2.10 Monitoring

2.10.1 All network and security devices should be monitored for security and performance level.

2.10.2 Security Monitoring

2.10.2.1 Network should be monitored for desired performance level and any unauthorized usage by the designated user.

2.10.2.2 Appropriate logging should be enabled on network/security devices for recording of security logs and logs for activities performed on network/security devices. Logging should be enabled taking into account the system capabilities and performance requirements.

2.10.2.3 Network/security devices should be monitored for security logs, user access logs, temporary user access and activity logs. Any security incident or abnormalities should be handled in co-ordination with ITSD.

2.10.2.4 All critical logs should be securely maintained at secondary storage for future reference.

2.10.3 Performance Monitoring

2.10.3.1 Performance Monitoring should be carried out by collecting and collating information in respect of bandwidth utilization, link status, CPU utilization, uptime of the links and devices etc.

2.10.3.2 Monitoring systems should be configured to alert the Network Administrator when the performance goes down below the acceptable levels via any trigger, e-mail, pop-up or SMS messages.

2.10.3.3 SLA with network link service providers should include the above performance parameters, committed bandwidth and penalties for non- performance. The SLAs should be monitored in accordance with the SLA Management Policy.

2.10.3.4 Periodic reports should be submitted to appropriate authority on results of Security and Performance monitoring activities.

2.11 Documentation

2.11.1 Branch/Department/Administrative Offices should maintain
detailed documentation of the network with following
details

- Network connectivity including Switches/Routers/Link speeds

- Firewalls

- Application Server details

- IP addresses

- Firewall (if any at the branch) rule base details

3 Operating System Security

3.1 Policy Statement

3.1.1 The most secure implementation of the operating system should be selected at installation time and user access to operating system should be restricted and monitored. Operating system should be kept current against security patches released by the vendor.

Standards and Procedures

3.2 Applicability

3.2.1 The policy applies to operating systems of all multi-user systems.

3.3 User authentication

3.3.1 User Access and Password Management policy should be referred for authentication of user, creation of user ID, assignment of privilege levels, password management, user access review, logging and related activities.

3.3.2 All users logging remotely on server should also be authenticated by Operating System before providing access. Remote login setting should be configured such as to allow access to authorized users only.

3.4 Security of user credentials

3.4.1 User login passwords should be stored and sent in encrypted format over the network.

3.5 Logging

3.5. 1 Logging should be enabled to track critical system activities. Logs provide the audit trail and play an important role in tracking malicious users in the event of a compromise. OS should be setup to log all security related events including the following:

- User account management
- User Privilege changes
- User login/logout time
- Changes in OS configuration
- Authentication failures
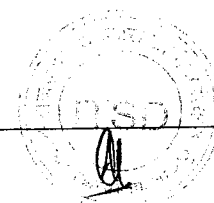
3.6 Patch Updation

ITSD is responsible for ensuring that all necessary security patches and hot fixes for the operating system are applied.

3.7 Anti-virus

3.7.1 Anti-virus software should be installed on the systems with risk of virus infection. All Microsoft operating systems should have anti-virus installed.

3.7.2 Anti-virus software should be updated with latest signature patterns. ITSD should ensure that anti-virus patterns are always current.

4 Database Security

4.1 Policy Statement

All database systems will be installed and configured to high security. Integrity and stability of databases must be maintained at all times. User access to database will be provided after authorization and authentication, based on job requirement.

The bank has outsourced the database management to our ASP M/S C-Edge Technology Pvt ltd, as we are totally depending upon database management on our ASP they have been instructed to ensure proper security of banks database by following the best industry practices.

5 Cryptographic Controls

5.1 Policy Statement

Encryption should be used for the Bank's sensitive information that will be stored in systems, media/device or accessed/transmitted over external/untrusted networks. Transmission of sensitive and confidential data with external parties should be authenticated by use of electronic/digital certificates. Secure processes should be employed for key generation, distribution, revocation and storage wherever electronic/digital certificates are used. Management of critical servers or security devices should be done over secure channel using encryption techniques.

Standards and Procedures

5.2 Secure storage of sensitive information

5.2.1 Cryptographic Controls should be used for ensuring the confidentiality and integrity of sensitive information stored on desktops/servers or movable or external storage devices or media including laptops, PDAs, CD/DVDs, to facilitate Data Loss prevention

5.3 Secure Transmission of data

5.3.1 Sensitive and confidential data should be encrypted when sent over external/untrusted networks or where higher degree of security is required. External networks refer to networks that are not directly managed by bank and include Internet, service provider networks and correspondent organizations.

5.3.2 User passwords should be encrypted when transmitted over internal networks including LAN and WAN. Other data sent over internal networks can be encrypted based on risk assessment.

5.3.3 If there is sensitive and confidential information that needs to be transmitted over internal network, applications owners need to consult Information Security Dept to analyze and determine the need for cryptographic controls.

5.3.4 Appropriate encryption methods for data in transit should include, but are not limited to, Transport Layer Security (TLS), Secure Socket Layer (SSL) 3.0, Secure Shell (SSH) 2.0, HTTPS etc.

5.3.5 Appropriate enterprise level infrastructure should be acquired and deployed for file transfer / sharing /exchange throughout Bank efficiently and securely by suitable functionaries.

5.4 Authentication of sensitive information

5.4.1 Communication of information classified as sensitive including transaction details should be authenticated by electronic signatures.

5.4.2 Only approved encryption standards including electronic signatures, digital certificates, and encryption utilities should be used by authorized users.

5.5 Encryption Standards

5.5.1 Data should be encrypted using asymmetric or symmetric keys. Symmetric encryption is faster compared to asymmetric. The exchange of key used for symmetric encryption should be conducted using asymmetric keys.

5.5.2 To limit the risk of unauthorized access, there should be provision for dynamically changing the keys used for encryption. If static keys are used these should be changed periodically.

5.5.3 Strong symmetric encryption algorithms including 3DES, AES, RC4 with minimum key length of 128 bits should be used.

5.5.4 Asymmetric keys should have minimum length of 1024-bit.

5.6 Key Management

5.6.1 Designated owner should ensure that following security measures are followed for Key Management in approved cryptographic technique:

5.6.1.1 Generation of strong cryptographic keys

5.6.1.2 Secure cryptographic key distribution

5.6.1.3 Secure cryptographic key storage

5.6.1.4 Cryptographic key changes for keys that have reached the end of their crypto-period.

5.6.1.5 If manual clear-text cryptographic key management operations are used, these operations should be managed using split knowledge and dual control

(for example, requiring two or three people, each knowing only their own key component, to reconstruct the whole key).

5.6.1.6   Prevention of unauthorized substitution of cryptographic keys.

5.6.1.7   Protect any keys used to secure critical information asset against disclosure and misuse.

5.6.1.8   Cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.

6 Monitoring

6.1 Policy Statement

All access to critical IT systems and applications and the Bank's network should be monitored for performance level and suspicious activities or security breaches and adequate response mechanism should be setup for controlling security breaches.

Standards and Procedures

6.2 Security Monitoring

6.2.1 Security monitoring of network and security devices' traffic to Bank's critical systems and applications should be performed through a centralized Security Operation Center (SOC), a dedicated set up for monitoring activities.

6.2.2 All critical application servers and network devices should be monitored for uptime.

6.3 Performance Monitoring

6.3.1 ASP are responsible for setting up systems for performance monitoring and alerting.

6.3.2 The performance statistics of all critical multi-user application servers etc should be continuously monitored. The parameters that need to be monitored include CPU, memory and disk space utilization. High levels of system resource utilization could be indicated if the system is under a denial of service attack or is performing some malicious activity.

6.3.2.1 For network devices, in addition to CPU and memory utilization, the link utilization also should be monitored.

6.3.3 ITSD should define acceptable usage levels for various parameters that are being monitored. For example for the critical servers at Data Centre the acceptable usage level for CPU could be 60%. If the CPU utilization exceeds 60% it could be an indication of some abnormal activity or higher peak load and should be reported and investigated.

6.3.4   Performance monitoring systems should be configured to automatically alert the System official if the performance exceeds acceptable levels. Alerting can either be over Email, SMS or pop-up messages.

6.4 Log Monitoring

6.4.1   Application owner should be responsible for setting up systems for collecting and analyzing the logs from respective applications, OS, database etc.

6.4.2   Logs from all security and monitoring devices including NIDS, HIDS and firewalls should be collected at centralized log server to enable centralized and comprehensive log monitoring by Security Operation Center.

6.4.3   Logging should be enabled on all the critical devices including application servers, network devices, operating system, database, web servers, and security devices. Date and time on all IT systems including network & security devices, servers, desktops, ATM machines in the Bank should be set correctly to reflect Indian Standard Time to enable successful correlation of logs across multiple systems. All critical systems should be time synchronized with GPS/internet-sync time server.

6.4.4   Logging should be enabled to capture audit trails of an event including following details:

   6.4.4.1   User or Process Identification

   6.4.4.2   Type of event

   6.4.4.3   Date and Time

   6.4.4.4   Details of event- Resource accessed like file, server, network device etc

   6.4.4.5   Success or Failure indication

   6.4.4.6   Origin of event

   6.4.4.7   Identity or name of affected data, system component, or resource.

   6.4.4.8   Access to audit logs or trails

6.4.5   Logs should be monitored for all activities that would affect the security level of the system including the following.

6.4.5.1   Authentication failures

6.4.5.2   Account created/deleted/disabled

6.4.5.3   Password change for privileged accounts

6.4.5.4   Changes in security configuration settings

6.4.5.5   Start and stop of service

6.4.5.6   System/Console alerts/errors or failures/fault logs.

6.4.5.7   Administrator or Root user activities

6.4.5.8   Access to audit trails

6.4.5.9   Creation and deletion of system-level objects

6.4.5.10   Alarms/alerts raised by the access control system

6.4.5.11   Details of system/application/files accessed.

6.4.6   Person(s) responsible for log monitoring should submit periodic reports to the application owner.

6.5 Log Protection

6.5.1   The log information and logging facilities should beprotected against tampering and unauthorized access.

6.5.2   Remote copy of log file should be maintained in secondary storage or log server for critical IT systems. Same should be protected for authorized read-only access.

6.5.3   Care should be taken with the appropriate controls to ensure that the log files are not altered while copying for secondary logs required for analysis, audit trails etc.

6.5.4   Failure to log the events due to overflow or over writing of past record events etc. should be prevented.

6.5.5   ITSD should classify the log records based on its relevance and importance in security events. Application Owner should also define the retention period for the same as per the Data Protection Policy.

6.6 Log Review

6.6.1   ASP should submit periodic reports to ITSD as per requirements set by the Bank from time to time, for review.

6.6.2 ITSD should define procedures for such review and reporting of any unauthorized events/exceptional activity to his controller for necessary actions.

6.6.3   ITSD should determine the retention period for log files in consultation with all the HODs and should ensure that retention periods are compliant with the Bank's policy for record retention.

7 Risk Management

7.1 Policy Statement

7.1.1 The Bank shall identify, analyze and mitigate risks which affect confidentiality, integrity and availability of information system assets.

Standards and Procedures

7.2 Risk Assessment Methodology

7.2.1 A risk assessment methodology should be identified that is suitable to the Bank and the identified information security, legal, statutory and regulatory requirements.

7.2.2 The risk assessment methodology should ensure that risk assessment produces comparable and consistent results.

7.3 Asset Identification and Classification

7.3.1 All assets should be identified by respective Dept heads and an asset inventory should be maintained. The asset may be of the following types:

- ☐ *Information Assets* that include data files, e-records, system documentation, user manuals, training material, operational procedures for IT management, software licenses, source codes, business continuity plans, contracts, guidelines, HR records etc as kept in electronic formats. Document in paper would also constitute Information Assets. Some of the examples include contracts, company documentation, business results, purchase document, invoices, license agreement, escrow agreements etc.

- ☐ *Software Assets* that include business applications, operating systems, databases, knowledge management application, development tools, utilities etc.

- ☐ *Physical Assets* that include servers, networking equipment, security devices, backup media, printers, biometric devices, server racks, desktops, laptops etc.

- ☐ *Services and Processes* that include computing, telecommunications, power, general utilities like air conditioning, alarm systems, fire prevention, hardware and application support etc.

□ *People Assets* that include Bank's employees.

7.3.3 All assets including hardware, software, physical assets, and media should be reviewed for risk assessment by respective HODs at least once in a year.

7.3.4 All information system assets of the Bank should be classified by the asset owner in consultation with ITSD based on their business value and impact to business operations.

7.3.5 Asset value should be based on level of three parameters i.e. Confidentiality, Integrity and Availability of that asset to Bank's business as High, Medium and Low. The highest value among three parameters should be assigned as Asset value. E.g. Confidentiality=High, Integrity=Medium and Availability=Medium, then asset value will be High, based on confidentiality level which is highest among three parameters.

7.3.6 The level of Confidentiality, Integrity and Availability should be valued in terms of business value and impact of Information System assets for continuance of business operations of the Bank as follows,

Classification	Description
High	High Value implies that the asset is critical to business and its unavailability, modification/degradation/damage and / or unauthorized disclosure can lead to a significant loss of business and the business cannot continue to perform its primary function in normal manner.
Medium	Medium value implies that the asset is critical to business and its unavailability, modification/degradation/damage and / or unauthorized disclosure can lead to a moderate impact to business as the business may continue to perform its primary function, but the effectiveness of the functions is significantly reduced.

Low	Low value implies that the asset is less critical to business and its unavailability, modification/degradation/damage and / or disclosure can marginally affect business as the business will continue to perform its primary function, but the effectiveness of the functions is minimally reduced.

7.3.7 Information may also be classified based on its sensitivity to business operations. Asset owner should classify the information in consultation with ITSD based on a defined scheme issued by ITSD. The Bank classifies information as one of the following,

Classification	Description
Public	Information that is available to the general public and intended for distribution outside the Bank. This information may be freely disseminated without potential harm.
Restricted	Information that is deemed sensitive due to financial or legal ramifications and which is for use only by authorized bank employees and auditors, consultants, vendor personnel, legal and regulatory authorities.
Confidential	Information that is proprietary to the Bank and its unauthorized disclosure could adversely impact the Bank, its employees and its customers.

7.3.8 ITSD may periodically review the classification given to the information or valuation of an asset based on changes in business environment.

7.4 Risk Assessment

7.4.1 Risk Assessment should be performed by ITSD, in consultation with HODs, by following three steps as briefed below:

7.4.1.1 **Risk identification** is to find, recognize, and describe the risks that could affect the achievement of objectives which should be met through an application.

7.4.1.2 **Risk analysis** is to understand the nature, sources, and causes of the risks that are identified and to estimate the level of risk. Risk analysis exercise should also study impacts and consequences and examine the controls that currently exist. Risk analysis is elaborated in subsequent clauses.

7.4.1.3 **Risk evaluation** compares the estimated risks, established by means of a risk analysis, with a set of risk criteria. This is done in order to determine how significant the risk really is i.e. whether level of risk is acceptable or not.

7.4.1.4 Guidelines on how to conduct Risk Assessment at branches/offices shall be issued by ITSD.

7.4.2 ITSD should identify various risks based on the identified threats and vulnerabilities and the impacts that losses of confidentiality, integrity and availability may have on the assets. Given below is a brief description on threat and vulnerability:

7.4.2.1 A threat is a potential cause of an incident that may result in harm to system or organization. Threats can originate from accidental or deliberate sources or events. Example: Unauthorized access to information, systems or software.

7.4.2.2 Vulnerability is a weakness of an asset or group of assets than can be exploited by one or more threats. The weakness could be exploited by threats causing unwanted incidents that might result in loss, damage or harm to these assets and the business of the organization. Example: No or weak password and account policy on systems, applications or database.

7.4.3 Threats are categorized as "High", "Medium", "Low" based on their likelihood of occurrence. The following table defines the threat levels,

Threat Level	Description
Low	Low likelihood. It is not likely that the threat will occur, there are no incidents, statistics, motives, etc. that indicate that this is likely to happen.

Medium	Medium likelihood. It is possible that the threat will occur, there have been incidents in the past, or statistics or other information that indicate that this or similar threats have occurred sometime before, or there is an indication that there might be some reasons for an attacker to carry out such action.
High	High likelihood. The threat is expected to occur, there are incidents, statistics or other information that indicate that the threat is likely to occur, or there might be strong reasons or motives for an attacker to carry out such action.

7.4.4   Vulnerabilities are rated as "High", "Medium", "Low" based on ease of exploit and level of protection currently present on the asset. The following table defines the vulnerability levels,

Level	Description
Low	Unlikely. The vulnerability is hard to exploit and the protection in place is good.
Medium	Possible. The vulnerability might be exploited, but some protection is in place.
High	Highly probable or probable. It is easy to exploit the vulnerability and there is little or no protection in place.

7.4.5   Risk assessment procedure of the Bank follows a zero-control approach for   the first time for new systems/applications. In this approach, all the threats and vulnerabilities a particular asset may be exposed to are identified and appropriate controls are selected to mitigate the vulnerabilities and the reduce risk to acceptable levels.

7.4.6   Afterwards, Risk assessment procedure should follow an ongoing approach for existing systems/applications. This approach takes into account all the existing controls and their effectiveness in terms of residual risks and assessment for new vulnerabilities and controls required.

7.4.7   The ranking of risks is based on a qualitative and quantitative method. Risk ranking is arrived based on following formula:

Risk Ranking = Asset value × Threat Value× Vulnerability Value

7.4.8 Values for Asset, Threat and Vulnerability are scaled as 3 for High, 2 for Medium and 1 for Low.

7.4.9 Threat includes the likelihood of occurrence of an incident.

7.4.10 The asset values and the threat and vulnerability levels are matched in a matrix as shown below. All the identified risks for the asset should be ranked based on the risk ranking matrix given below,

	Threat Level	Low			Medium			High		
	Vulnerability Level	L	M	H	L	M	H	L	M	H
Asset Value	Low	1	2	3	2	4	6	3	6	9
	Medium	2	4	6	4	8	12	6	12	18
	High	3	6	9	6	12	18	9	18	27

7.5 Risk Acceptance Level

7.5.1 Based on the above matrix the risks can be ranked on a scale of 1 to 27. For example, if the asset has the value "medium", the threat is "high" and the
vulnerability is "low" the measure of risk in this case would be "6". The Bank has decided a risk value of 0 – 9 as acceptable and any risk having a value between 10– 27 needs to be mitigated to bring down the risk level.

7.5.2 The ITSD in consultation with HODs should conduct a risk evaluation to determine whether risks are acceptable or require treatment. The risk evaluation should be conducted in terms of the business impact and probability of occurrence in the context of existing controls. Asset owner should document the same in a Risk Assessment report.

7.5.3 Risks that are above the acceptable level qualify for the risk treatment. Controls should be determined and approved by ITSD. The selection of controls should take into account the business, legal, statutory and regulatory requirements.

7.6 Risk Treatment

7.6.1 Risk Treatment is the overall responsibility of the ITSD and it should implement controls identified in the risk analysis phase in order to mitigate the risk.

7.6.2 ITSD should prepare a Treatment Plan that outlines the roadmap for implementing the selected controls. Treatment plan should identify the limiting factors, dependencies, priorities, resource requirements, mile stones and approval of allocation of resources.

7.7 Residual Risk

7.7.1 The asset owner should measure the residual risk after implementing the controls. Residual Risk is the risk that remains even after risk treatment. This may be due to cost of implementation is higher than the potential loss. If residual risk level is above Risk Acceptance level (9) after risk treatment, the decision to accept the risk should be taken by Chairman. Whenever control cannot be identified or cost of implementation outweighs the potential loss, a decision can be taken to accept the risk. In such scenario, the decisions should be documented properly.

7.8 Continuous Monitoring and Review

7.8.1 The ITSD should undertake reviews at regular intervals to verify the adequacy of existing controls, residual risk and acceptable level of risks. The ITSD should monitor the implemented controls, measure the control effectiveness.

7.8.2 The ITSD should identify any new risks arising due to significant changes made to the assets or business processes.

8 Data Protection

Policy Statement

8.1.1 All identified data shall be protected in all phases of its life cycle including collection, processing, transmission, storage, exchange and retirement. Privacy of Personally Identified Information of the Bank shall be ensured.

Standards and Procedures

8.1 Data Identification

8. 2.1 Officials, designated for protection of data as per this policy, shall identify the Bank's data in following lines:

8.2.1.1 Business Data

8.2.1.1.1 Business data refers to information proprietary to the Bank which includes financials records, sales, marketing, and products data.

8.2.1.2 Personally Identifiable Information

8.2.1.2.1 All data which can uniquely identify an individual, either Bank's customer or employee, is called as Personally Identifiable Information (PII).

8.2.1.2.2 PII of an individual may include following but not limited to:

- Name, like full name, maiden name, mother's/father's maiden name

- Personal Identification Number like PAN, Passport Numbers, Driving License, Voter id, aadhar etc.

- Address information e.g. residential address, office address, email address etc.

- Contact numbers e.g. LL/Mobile number, business or residential phone number

- Personal characteristic e.g. photographs, fingerprints or other biometric data

8.2.1.2.3 Information about an individual that is linked to one of the above like date of birth, place of birth, employment information, medical history information, financial information (debit card numbers, Bank account numbers)

PII which is explicitly required for a business purpose should only be collected from the individuals. All such data should be ensured for its accuracy, authenticity, completeness and updation on regular basis by respective Information Owner.

8.2 Roles and Responsibilities for Data Protection

8.3.1 Group Executive as Information Owner

The Chairman shall be the Information Owner and shall be responsible for respective Bank's business information asset. Responsibilities would include, but not be limited to:

8.3.1.1 Nominate Information sub-owners for each Business unit

8.3.1.2 Assigning business information classification and periodically reviewing the classification to ensure it still meets business needs

8.3.2 Business Head as Information Sub-owner

The General Managers shall act as Information Sub-Owner and shall be responsible for following in co-ordination with respective HODs:

8.3.2.1 Ensuring security controls are in place commensurate with the classification

8.3.2.2 Reviewing and ensuring currency of the access rights associated with information assets they own

8.3.2.3 Determining security requirements, access criteria and backup requirements for the information assets they own

8.3.3 Data Protection Officer

Data Protection Officer (DPO) shall be the Head of Dept/Branch-Head for protection of information managed with respective unit.

8.3.3.1 As DPO, he/she shall be responsible for implementation of this policy for Data Identification and Data Inventory Management.

8.3.3.2 DPO should maintain a Data Distribution list, of all identified data, having details of users who have been approved for access of these data. Details should include User, Data and Access Time Period.

8.3.4 User manager

The user manager is the immediate manager or controller of an employee. He/she has the ultimate responsibility for all user IDs and information assets

owned by Bank

employees. In the case of non-employee individuals such as contractors, consultants, etc., user manager is responsible for the activity and for the Bank assets used by these individuals. Responsibilities include the following:

8.3.4.1 Informing application owner of the termination of any employee within his unit so that the user ID owned by that individual can be revoked, suspended or made inaccessible in a timely manner

8.3.4.2 Informing application owner of the transfer of any employee if the transfer involves the change of access rights or privileges

8.3.4.3 Reporting any security incident or suspected incident to the Information Security function

8.3.4.4 Ensuring that employees are aware of relevant security policies, procedures and standards to which they are accountable

8.3.5 End user

The end users shall be any employees, contractors or vendors of the Bank who use information systems resources as part of their job. Responsibilities include:

8.3.5.1 Maintaining confidentiality of log-in password(s)

8.3.5.2 Ensuring security of information entrusted to them as a part of job responsibility

8.3.5.3 Using Bank business assets and information resources for management approved purposes only

8.3.5.4 Adhering to all information security policies, procedures, standards and guidelines

8.3.5.5 Promptly reporting security incidents to management.

8.3.6 Application Owner

Application Owner, as Information Custodian, is the delegate of the information owner with primary responsibilities for dealing with **management of information systems** providing business functions and having related business information. Responsibilities include, but are not limited to, the following:

8.3.6.1 Implementation of security controls according to information classification assigned by business owner

8.3.6.2 Establishing user access criteria, availability requirements and audit trails for their applications

8.3.6.3 Ensuring security controls associated with the application are commensurate with support for the highest level of information classification used by the application.

8.3.6.4 Performing or delegating the following:- day-to-day security administration, approval of exception access requests, appropriate actions on security violations when notified by the security administration, the review and approval of all changes to the application prior to being placed in the production environment, and verification of the currency of user access rights to the application Management of information system and ensuring data protection.

8.3.7 IT Department

The IT cell shall be responsible for day-to-day operational management of information systems and administration of user IDs and access rights. Apart from operational activities, their data protection responsibilities include the following:

8.3.7.1 Performing backups according to the backup requirements established by the information owner

8.3.7.2 When necessary, restoring lost or corrupted information from backup media to return the application to production status

8.3.7.3 Ensuring record retention requirements are met based on the information owner's requirements.

8.3.7.4 Support to business units for any information required by them

8.3.7.5 Ensuring access requests are consistent with the information directions and security guidelines

8.3.7.6 Administering access rights according to criteria established by the Information Owner

8.3.7.7 Creating and removing user IDs as directed by the user manager

8.3.7.8 Administering the system within the scope of their job description and functional responsibilities

8.3.7.9   Reporting and following up on security violation reports

8.3.8   Chief Information Security Officer

Chief Information Security Officer (CISO) shall be responsible for:

8.3.8.1   Consulting the HODs for implementation of appropriate security controls and regular review of implementation of the same.

8.3.8.2   Understanding different data environments and the impact of granting access to them

8.4 Data Inventory Maintenance

8.4.1   An inventory should be maintained of identified data (categories of data) along with following information: Data name, DPO, Data storage location, Data Classification, Business Justification of Data collection/storage, Data Retention period and Data retirement and disposal dates. The inventory should be reviewed periodically by respective DPO.

8.5 Data Protection Controls

Following controls should be implemented for the protection of data:

8.5.1 Access to data should be provided controlled based on classification of data and need to know basis.

8.5.1.1   It should be ensured that application outputs are reviewed so that no excess information is revealed and only information that is required to perform the job responsibilities are available to users.

8.5.1.2   Segregation of Duties should be implemented with applications and regular business/ IT processes to ensure integrity and confidentiality of data. Bank's IT and IS Policy on Segregation of Duties, Change Management should be referred.

8.5.2 Access to data should be provided only for defined time period as per business requirement, and access should be removed/ disabled after such duration.

8.6 Data Storage

8.6.1 Data Storage and Retention should be done with measures adequate to its classification.

8.6.2 Confidential data should only be stored in locations which are approved by DPO.

8.7 Data Exchange and Disclosure

8.7.1 A Non-disclosure agreement should be signed prior to exchanging data with third parties or entities other than the Bank.

8.7.2 Incase data is being exchanged through some courier agencies, a list of authorized courier agencies should be approved by Bank and a procedure for selecting those agencies should be in place. Bank should ask courier agencies to sign a non-disclosure agreement.

8.7.3 All information security requirements must be defined clearly in the service agreement with third-party for data protection.

8.8 Monitoring and Review

8.8.1 All access to, modification or deletion of data by users should be logged. Logging methods and levels should be decided based on data classification.

8.8.2 All privileged access to data stores should be logged and monitored. These should be reviewed by overseeing authority on regular basis.

8.8.3 Any suspicious use of data / security incident should be handled as per the Bank's IT and IS Policy on Incident Management.

8.8.4 Classification should be reviewed, atleast once in a year and whenever classification changes to ensure the categorization/classification fulfill current business need.

8.8.5 Bank should conduct annual compliance audit to verify compliance to this policy and applicable legal, regulatory and industry requirements for data protection.

8.8.6 IS audit should be carried out to verify the effectiveness of security controls implemented to protect Bank's data.

9 Wireless Security

9.1 Policy Statement

Wireless Networks, both in Local Area Network (LAN) and Wide Area Network (WAN) environments should be configured and operated in a secure manner. Use of Wireless Network Technology in the Bank should be done only after ensuring all security requirements are met and approved by CISO. Wireless Network Setup should have controls to ensure confidentiality, integrity and availability of the information transmitted over the wireless network. Wireless Network should be protected against eavesdropping, man-in-the- middle attacks, data modification and resource misappropriation, denial of service etc. Wireless Network should be monitored to ensure the continuous availability to authorized users only.

Standards and Procedures

9.2 Use of Wireless Network in Bank

9.2.1 As part of Bank's overall Network redesign or Technology Refresh, if it becomes necessary to have a large number of wireless links, Bank should lay down standard procedures to be complied with by the services providers.

9.2.2 Wireless Network as a part of Local Area Network (LAN) should not be deployed at branches.

9.2.3 For administrative offices, Wireless network setup should be considered for approval in the following situations:

- if wired network is not feasible; or

- for redundancy purposes; or

- in all other cases, deployment of wireless network should be considered only after a specific approval from CISO on the recommendation of ITSD.

9.2.4 IT- Dept should carry out site specific risk assessment before granting approval for wireless deployment. The risk assessment should include the following:

- Location for wireless network setup

- Applications to be accessed by the proposed installation

- Outsourcing risks including the local vendor, if any

9.2.5 Unauthorized wireless network should not be used in the Bank.

9.3 Wireless Technology: Deployment considerations

9.3.1 IT- Dept should examine various alternate secured technologies in comparison to any wireless technology before approval. Wireless Technology should not be used if alternate secured technologies are available, unless business need can't be served without wireless technology.

9.3.2 Wireless technology should be discouraged for normal routine operations including accessing internet, voice communication.

9.3.3 Use of any non-approved wireless technology e.g. Bluetooth is prohibited in the Bank. IT-Networking Dept should maintain a list of all approved wireless technologies in the Bank.

9.4 Wireless Network Management & Monitoring

9.4.1 IT- Dept is responsible for overall management of wireless network(s).

9.4.2 Any User/device which requires access to the Bank's wireless network should be permitted by IT –Department.

9.4.3 IT- Dept should maintain a central record of all wireless connections and its related infrastructure.

9.4.4 Where possible, wireless devices used in WAN should be switched off when not used or required, such as after office hours or holidays.

9.4.5 Connectivity to internet through wireless modems such as internet data cards, mobile phones, etc. should not be allowed to the system connected to LAN network. The Acceptable Usage Policy should also be referred in this regard.

9.4.6 Periodic review should be conducted to ensure that the wireless network is not accessible outside the identified area and no unauthorized wireless access points are used. It should be ensured that the authentication key for the wireless network is with ITSD only and should be provided to the authorized users only.

9.4.7 All wireless clients, which are used to access critical networks or handle Bank's data, should be configured in such a manner that they cannot be used to connect to public wireless networks or any other networks beyond those specifically allowed by the Bank.

10.0 Email Usage

- Bank's electronic mail system should be used for Bank's business communication.
- Use of Bank's official mail account for personal purposes is discouraged.
- Due to its ease of use, faster and efficient communication and to save papers, emails are used for –
    - a. Day to day communications
    - b. Intra-office (within branch / office / dept) and inter-office communications
    - c. Communication to and from customers
    - d. Important instructions / communications from administrative offices
- Users owning the email account are fully responsible for the content of email originated, replied or forwarded from their account to other users within or outside the Bank.
- Email sent from Bank provided email ID is as good as letter on Bank's letter head.
- Bank may intercept or disclose or assist in intercepting or disclosing Email communications to ensure that email usage is as per Bank's IS Policy. User communications should not be considered private as also not send inappropriate contents.
- Inappropriate contents include contents that –
    - a. Are libellous, defamatory, offensive, racist, Anti-National messages, obscene remarks or for private business activities, personal gain or profit or job search
    - b. May damage the reputation of the Bank, contain viruses, worms or malware
    - c. Chain mails containing virus hoaxes or for charitable fund raising campaigns, political advocacy efforts, religious efforts, or personal amusement and entertainment and others.
    - d. Unsolicited emails to large number of users which can be considered as mail spamming.
    - e. Using email system to copy and/or transmit any document, software or other information protected by copyright or any other law.
    - f. Mails to external entities containing instructions or contents that require authorization of a superior in the normal course of Banking, unless such prior authorization is obtained.
- Confidential or secret information should be encrypted or password protected when transmitted over email. It is recommended to start subject line with "Confidential", "Secret", "Private & Confidential", "Internal" and then mention subject. It then becomes responsibility of recipients to ensure confidentiality / privacy of the matter reported.

- Don't provide Bank's email account to any mailing lists / internet websites / Internet newsgroup / discussion board. These websites, persons might provide your email ID to

their interested parties and likewise the email ID would get circulated to number of unknown people / entities.

- Providing email ID like above might result into receiving emails like marketing, lottery, draws, phishing etc. called SPAM unnecessarily flooding inbox with no space left for official emails.

- Do not open / download attachments from emails howsoever appealing they are, if email is from unknown sender or even the attachment is not expected from known person / official.

- These attachments might drop virus, worms, Trojans, Botnets into the system and transmit data / information in bits and pieces to the hacker.

- The contents like photo, video etc. in email attachments might also contain hidden messages behind them which cannot be seen in normal course. This technique is called Steganography technique (used by terrorist, defence, secret services). The user responsible for creating / forwarding such emails could be held responsible.

- Trojans like Advance Persistent Threat – APT attack have resulted into financial and IPR losses to companies, embarrassment and action on officials responsible for the compromise.

- The malware infection can also make the system Zombie (of which owner is unaware) and forward transmissions (including spam or viruses) or launching DDoS attack on other computers on the Internet. Such system is controlled by Master (called BotNet Command & Control – C&C) system unknown to user.

- Users should not access Bank's email account from insecure internet connection like open Wi-Fi, public hotspots, insecure cybercafe etc.

- Users should promptly report all suspected security vulnerabilities that they notice with the Email account to authorized personnel.

- Bank should ensure implementation of Anti phishing, Anti Malware, DMARC, DKIM and SPF controls for the mail domain.

How to identify SPAM email?

- When the email id, contact information is given on various websites, surveys, conferences, hotels, magazines etc. they might share the same with their partners, their sister concerns and likewise the chain gets extended without any limit. These email IDs and contact information might land in unscrupulous elements (domestic and foreign) and thus get added in emailing / SMS list. Thus people whose contact information gets into their hand, would start receiving various offers via emails / SMS and even social engineering emails like Phishing etc.

- SPAM emails are unsolicited bulk email and sent to numerous recipients informing potential victim about having won lottery, receipt of Goods, recruitment, custom clearance, business partnership, update Bank account information due to security reasons etc.
- Typically, spam email would have no email ID in "To" or "CC"
- As the spam is sent to billions of recipients, it would not be addressed specifically to recipient / victim. Instead of Dear Sh. Makarand, it would address recipient as "Dear RMGB Customer", "Dear Valued Customer" etc.
- It would encourage the recipient to click on a Link or open an attachment which could lead victim to Phishing Site or download virus, Trojan etc.

Types of Email IDs and their purpose

- There is different type of email addresses allotted to the branches, offices &services along with KRA based Email IDs.
- Email address provided to branches like rmgb.0025@rmgb.in
- Designation / Role based email address provided like gm1@rmgb.in
- New incumbent (email id owner) should immediately change password of such email id after assuming charge of seat / office.

11.0 Patch Management Policy

11.1 Purpose:

The purpose of this policy is to ensure that all systems and software within the organization are patched in a timely manner to mitigate the risk of security vulnerabilities.

The hardware having computers and applications should be frequently patched to protect against widespread worms, malicious code that target known vulnerabilities on non-patched systems, resulting in downtime & business impact on bank.

The down time and business impact can be avoided by have effective patch management which will keep updated the IT system and applications deployed in the bank.

11.2 Definitions

- Patch: A software update that addresses a security vulnerability or other issue.
- Vulnerability: A weakness in a system or software that could be exploited by an attacker.
- Risk: The likelihood and impact of a security vulnerability being exploited.

11.3 Scope

This policy applies to all systems and software within the organization, including:

- Operating systems
- Applications
- Software development tools
- Hardware devices

11.4 Deployment

Patches will be deployed to production systems in a timely manner.

11.5 Monitoring

The effectiveness of the patch management process will be monitored on an ongoing basis.

11.6 Auditing

The patch management process will be audited on a regular basis to ensure that it is being followed.

12 Glossary

12.1 Abbreviations

CAT : Central Anti-Virus Team
CCC : Change Control Committee
CCIT : Corporate Center IT
CERT : Computer Emergency Response Team
CET : Central Email Team
CFT : Central Firewall Team
CMT : Central Monitoring Team
CVC : Central Vigilance Commission
DCM : Data Centre Manager
DMD & : Deputy Managing Director & Chief Information Officer
CIO
DMZ : De-Militarized Zone
DR : Disaster Recovery
GUI : Graphical User Interface
HTTP : Hyper Text Transfer Protocol
IPR : Intellectual Property Rights
IS : Information Systems
ISD : Information Security Department
ISSSC : Information Systems Security Standards Committee (succeeded in
        2012 by ISC)
ISC : Information Security Committee
IT : Information Technology
LAN : Local Area Network
NDA : Non Disclosure Agreement
PKI   Public Key Infrastructure
SCD : Secure Configuration Document
SLA : Service Level Agreement
SQA : Software Quality Assurance
SRS : Software Requirement Specifications
UAT : User Acceptance Test
UCO : User Control Officer
URL : Universal Resource Locator
URS : User Requirement Specifications
WAN : Wide Area Network
OWSAP : Open Web Application Security Project
CISO : Chief Information Security Officer

12.2 Definition of Terms

Acceptance Testing : Formal testing conducted to determine whether or not a

system meets the requirements specified in the contract
or by the user. This testing enables the user to determine
whether or not to accept the system.

Access Control : The process of limiting access to the resources of an IT
asset only to authorize users, programs, processes,
systems or network.

Accuracy : A qualitative assessment of correctness, or freedom from
error in data processing

Alert :Alerts are often derived from critical audit events. They provide
notice of specific attacks directed at IT assets.

44

Anonymous Login	:	Services may be made available without any kind of authentication. This is commonly done, for instance, with the FTP protocol to allow anonymous access.
Application	:	A software package designed to perform a specific set of functions that is relevant to business, such as accounting, transaction processing or communications.
Application owner	:	Person having overall responsibility for application security in all activities related to design, development, deployment and support
Audit Trails	:	In computer security systems, a chronological record of system resource usage. This includes user login, file access, other various activities, and whether any actual or attempted security violations occurred, legitimate and unauthorized.
Authentication	:	To verify the identity of a user, device, or other entity in a system, often as a prerequisite to allowing access to resources in a system
Authorization	:	The granting of access rights to a user, program, or process. Usually, authorization is in the context of authentication. Once you have authenticated a user, the user may be authorized different type of access.
Authorized User	:	A user that has been granted permission, with clear limitations, to access information and systems.
Availability	:	The ability to use or access IT resources by authorized users as required. The property relates to the concern that information systems are accessible when needed and without undue delay.
Backdoor	:	Hidden software or hardware mechanism used to circumvent security controls or provide a way to access a computer other than through a normal login.
Banner	:	Display that appears on an information system to notify the user of conditions and restrictions governing system or data use.
Biometrics	:	Automated methods of authenticating or verifying a user based on physical or behavioral characteristics.
Black Box Testing	:	A method of verifying that software functions perform correctly without examining the internal program logic.
Branch Manager	:	Denotes heads of branches irrespective of designation in Bank
Branches	:	Also includes IT processing centers like SOC, MICR, GLS, CMP
Breaches/ Compromise	:	Bypassing of security controls which could result in disclosure or damage of information systems. A violation of controls of a particular information system such that information assets or system components are unduly exposed.
Buffer Overflow	:	This happens when more data is put into a buffer or holding area than the buffer can handle. This is due to a mismatch in processing rates between the producing and consuming processes. This can result in system crashes or the creation of a back door leading to system access.
Bugs	:	Any defect in the software that affects its functionality or

45

Computer Fraud	:	Computer-related crimes involving deliberate misrepresentation or alteration of data in order to obtain something of value.
Computer related positions of trust	:	Includes system administrators, network administrators, database administrator, facilities management personnel for critical applications like Core Banking, , SBI Connect, etc and persons having rights to create/ modify users on such applications.
Confidentiality	:	The assurance that information is not disclosed to inappropriate entities or processes. Confidentiality is defined as ensuring that information is accessible only to those authorized to have access.
Configuration	:	In configuration management, the functional and physical characteristics of hardware or software as set forth in technical documentation by election of one of the sets of possible combinations of features of a system.
Cookies	:	Data exchanged between an HTTP server and a browser (a client of the server) to store state information on the client side and retrieve it later for server use.
Corporate Center IT	:	Refers to all IT departments reporting to DMD & CIO.
Credit check	:	Verification of pecuniary liability of the person being recruited/engaged by way of declaration by the person himself and by reference to former employer.
Critical Information Asset	:	All information assets whose unavailability, modification/degradation/damage and / or unauthorized disclosure can lead to a significant loss of business and the business cannot continue to perform its primary function in normal manner eg. Core Banking, ATM, Internet Banking, Payment Systems, Mobile Banking, Data Centre, Treasury.
Cryptography	:	Science that provides the means, methods, and apparatus for converting plain text messages into secret messages and vice versa.
Data Integrity	:	The property that data has not been altered or destroyed or lost in an unauthorized or accidental manner.
Default Account	:	A system login account (usually accessed with a user name and password) that has been predefined in a manufactured system to permit initial access when the system is first put into service.
Denial Of Service	:	Any action or series of actions that prevents any part of a system from functioning in accordance with its intended purpose. This includes any action that causes unauthorized destruction, modification, or delay of service.
Dial-Up	:	The service whereby a computer terminal can use the telephone to initiate and effect communication with another computer.
Digital Certificate	:	The electronic equivalent of an ID card that authenticates the originator of a digital signature.
e-Records		Information recorded in a form that requires a Computer or other machine to process it.
Effectiveness	:	In security evaluations, an assurance of how well the applied security functions and mechanisms working

46

Employee	:	Refers to supervising, award and subordinate staff employed in the Bank.
End-User/ User	:	Person using application or computer networks for business purposes as opposed to system management purposes. Could be employee of the Bank, customers or partners of Bank.
Environmental Threats	:	Threats caused by environment including fire, humidity, dust or air borne particles, power fluctuations, temperature, flood, earthquake etc.
Exploit	:	To take advantage of a vulnerability in a system to gain access to system or to compromise the system
Fallback Arrangements	:	In the event of failure of transactions or the system, it is the ability to fall back to the original or alternate method for continuation of processing.
Firewall	:	A security software or hardware that sits between two networks and restricts data communication between the networks and thus protects one network against threats from the other network
Functionality	:	Describes features of the IT asset that support the business processes.
Gateway	:	Interface between networks that facilitate compatibility by adapting transmission speeds, protocols, codes, or security measures.
Hoax	:	In virus terms, an Email that warns of an invalid viral infection or risk, causing unnecessary concern to Email users.
Impersonation	:	An attempt to gain access to a computer system by posing as an authorized user.
Information Security	:	Measures that protect information systems by ensuring their availability, integrity, and confidentiality.
Information System	:	The entire IT asset, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information.
Interoperability	:	It is the capability of systems to communicate with one another and to exchange and use information including content, format, and semantics.
Intrusion	:	A deliberate or accidental set of events that potentially causes unauthorized access to an information technology (IT) system.
Intrusion Detection System	:	A security system that monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warning of attempts to access system resources in an unauthorized manner.
IT Assets	:	IT Asset equates to any computerized system or component thereof and thus includes software, hardware, media, data, databases and associated communications networks.
IT Service	:	The services provided by information systems to business users including the maintenance and provisioning of applications, network and data processing.
IT Solution	:	Refers to any hardware, software or service or any combination of these related to information technology
Least Privilege	:	Feature of a system in which users are granted the Least

permission possible in order to perform their tasks.
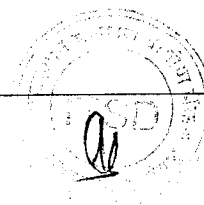
Lockout	:	The action of temporarily revoking network or application access, normally due to repeated unsuccessful logon attempts.
Login	:	The act of gaining access to a system; usually accomplished by providing a user name and password to an access control system that authenticates the user.
Malicious Code	:	Software that is intentionally included or inserted in a system for a harmful purpose e.g. A virus, worm, Trojan
Material Outsourcing	:	horse, or other code-based entity that infects a host.. Material outsourcing arrangements are those, which if disrupted, have the potential to significantly impact the business operations, reputation or profitability.
Media	:	Short for storage media: physical objects on which data can be stored, such as hard disks, CD-ROMs, floppy
Mobile Code	:	disks, and tape. Mobile code is software transferred between systems, e.g. transferred across a network or via a USB flash drive, and executed on a local system without explicit installation or execution by the recipient. Examples of mobile code include scripts (JavaScript, VBScript), Java applets, ActiveX controls, Flash animations, Shockwave movies (and Xtras), and macros embedded within Microsoft Office documents.
Modem	:	A device or application that permits a computer to transmit/receive data over telephone lines
Network Device	:	A device that is part of and can send or receive electronic transmissions across a communications network. Network devices include: end-system devices such as computers, terminals, or printers; intermediary devices such as bridges and routers that connect different parts of the communications network; and link devices or transmission media.
Non-Repudiation	:	A cryptographic service that legally prevents the originator of a message from denying authorship at a later date. A security service by which evidence is maintained so that the sender of data and recipient of data cannot deny having participated in the communication.
Operational Controls	:	Refers to control measures for checking the accuracy and reliability of information processing and means to prevent and correct errors in processes.
Outage	:	The period of time for which a communication service or an operation is unavailable.
Outsourcing	:	Provision of services by third party under contract which is of longer duration including maintenance, development, implementation, management or data processing services under the supervision of the Bank.
Patches	:	Small updates to software to address the bugs
Privilege	:	An authorization or set of authorizations provided on applications or network and governs the level of access of the user
Procedures	:	Procedures are detailed guidelines of how to implement the security controls and who should be responsible for the implementation.
Project Head	:	Person in charge of development/implementation of

		major IT solutions.
Proxy	:	A software agent that acts on behalf of a user, typical proxies accept a connection from a user, make a decision as to whether or not the user or client IP address is permitted to use the proxy and then completes a connection on behalf of the user to a remote destination.
Quality Assurance	:	A planned and systematic pattern of all actions necessary to provide confidence that products and services conform to established technical requirements, and that satisfactory performance is achieved.
Redundancy	:	Duplication of system components (such as hard drives, power sources, or processors), information (such as backup copies of software or archived files), or personnel intended to increase the reliability or availability of service and/or decrease the risk of information loss
Regulatory Requirement	:	Requirements prescribed by regulators of the Bank - RBI, Ministry of Finance, SEBI etc.
Reliability	:	The extent to which a system can be expected to perform its intended function with required precision.
Remote Access	:	Dial-up access by users through a modem for access to the computer network.
Residual Risk	:	Residual Risk is the risk that remains even after risk treatment. This may be due to cost of implementation is higher than the potential loss.
Risk	:	Risk is a situation with probability of exploitation of vulnerability by threat(s) resulting in negative impact once occurred. .
	:	.
Risk Management	:	The total process of identifying, controlling, and mitigating IT system-related risks. It includes risk assessment; cost benefit analysis; and the selection, implementation, test and security evaluation of security controls.
Safeguards/ Security Controls	:	Management, operational, and technical measures prescribed for an IT system which, taken together, satisfy the specified security requirements.
Sanitized data	:	Data taken from production environment and then

confidential information like customer information or

revenue information is masked or changed before using in test environment.

Security Policy	:	Includes IT Policy, IS Policy, Standards, Procedures and Guidelines
Security Weakness	:	Security Weakness is the vulnerability in the system which may be harmful to the system or its operations, especially when this weakness is exploited by a hostile agent or when it is present in conjunction with particular events or circumstances.
Scalability	:	The ability to move application software source code and data into systems and environments that have higher performance requirements without significant modification.
Sniffing	:	The unauthorized interception of information through tapping of wire or network over which the information is flowing.
Social Engineering	:	Attacking or penetrating a system by employing confidence tricks on users, rather than by means of a technical attack.
Software Escrow	:	Keeping the source code of software with a neutral third party with joint rights of vendor & Bank. In the event of vendor going out of business or not supporting the software, the code can be released to Bank.
Spam	:	To indiscriminately send unsolicited or inappropriate messages, especially commercial advertising in mass quantities.
Spoofing	:	A type of attack in which the attacker steals a legitimate network (e.g. IP) address of a system and uses it to impersonate the system that owns the address.
SSH	:	A protocol for secure remote login and other secure network services over an insecure network.
Standards	:	Standards define the specific requirements for meeting the policy objectives and include both technical and non-technical measures
Statutory requirement	:	Requirements mandated under legislative acts or law of the land.
Stealth Rule	:	A stealth rule is a rule which disallows any communication to the firewall itself from unauthorized networks/hosts. It is a rule to protect the firewall itself from attacks.
System official	:	Refers to IT personnel responsible for administration of routine system activities of servers, desktops, network and applications.
System Operations	:	Systems Operations refers to a team, or possibly even a group within the IT department/ wing, which is responsible for the running of the centralized systems and networks.
System Room	:	All areas which host servers or network equipment like system rooms in branches, CAP etc
Third Party	:	Visitors, on-site and off-site contractors, hardware and software vendors, repair personnel, technical support staff, ex-employees, temporary workers, cleaning and

Threat	:	Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, or denial of service.
Transition	:	Refers to the period in outsourcing where the process or set of activities is being taken over from one party by other party
Trojan horse	:	A malicious program, such as a virus or a worm, hidden in an innocent-looking piece of software, usually for the purpose of unauthorized collection, alteration, or destruction of information.
Upgrade	:	The process of replacing a version of software or hardware with a newer product release designed to meet new requirements, or generally improve performance.
User department	:	Refers to the Dept that is the user of IT application and IT services.
User ID	:	Unique symbol or character string used by a system to recognize a specific user.
Vulnerability	:	A weakness in system security procedures, system design, implementation, internal controls, etc, that could be exploited to violate system security policy.
White Box Testing	:	Testing of software for security features by evaluating its internals including design/ architecture and code.
Worm	:	An independent program that replicates complete copies of itself from machine to machine across network connections, often clogging networks and information systems as it spreads.

***************End of Document****************