Version 3.0 (Jan 2020)

Version History

Ver. No.	Ver. Date	Revised by	Description	Filename
1.0	01/04/2017	MG Compliance Team	Macro IT Security Policy	Macro IT Security Policy 2016_17- Revised.doc
2.0	04/01/2019	MG Compliance Team	Macro IT Security Policy	Macro IT Security Policy 2019-Revised.doc

Table of Contents

1. Background

Information is used in every aspect of our business, from processing payments to making investment decisions. It is an important and valuable asset for every organisation and needs to be suitably protected from a wide range of threats in order to ensure confidentiality, integrity and availability and to minimise business losses. It is therefore every organisation's policy to maintain a suitable set of controls and procedures to achieve an appropriate level of information security.

Continuous changes in technology and the business environment requires organisation to constantly improve business processes and to make them more effective and efficient. The ability of technology to meet these needs has transformed Information Technology ('IT') from a support function to an integral part of core processes spanning across all business functions and processes.

In line with the above we are taking IT Security seriously. We have developed and implemented the following products in various SME banks in the City under the company name Macro Infotech Limited with the brand name Macro Global (MG). Our Product and services portfolio covered as follows,

- Online Banking Application (View and Transaction based)
- Mobile Banking Application
- Mobile based Net Remit Application
- Remittance Services (Online based delivery channels)
- Trade Dealing System Middleware
- Online Deposit Taking Product
- Swift Message Management
- Faster Payment (inward and outward) and BACS Settlement system and Middleware
- Debit Card Management System
- Report Miner product to provide data warehousing
- Online Account Opening
- Document Management System for Scanning/ Indexing of all Physical Documents
- Regulatory Reporting and Compliance (SCV, CRS, FATCA, CIFAS, BBSI, PSD2, MIFID2, SFTR, CDAC)

To support these systems, we are procuring;

- Desktop Computers/ Servers/ Laptops/ Printers
- Networking and Telephone lines
- Virtual Servers for testing
- Internet connectivity
- Cloud Solutions

We have migrated to UK based Microsoft Azure Platform for our entire Product Research, innovation and development platforms with Enterprise level Mobile Security with score card of 70 points check across our process.

2. Introduction to Information Security Policy

This document is the information Security Policy of MG. It consists of concise and practical series of statements, management's views and position regarding information security for MG specific requirements.

Applicability of the Policy

This Policy applies to MG including its Employees, Business Alliance Partners, contractors, consultants, temporary staff and Third Parties, who have access to its Information/data/ Information Processing Facilities. All the employees and external parties as defined in policy are responsible to ensure the Confidentiality, integrity and availability of MG's information assets.

Scope

Information Security Policy is applicable to all Information and IT assets of MG that are electronically stored, processed, documented, transmitted, printed/ faxed.

Ownership

The Board of Directors MG is the owner of this policy and ultimately responsible for information security.

Staffing

The information security function is to be adequately resourced in terms of the number of staff, level of skills and tools or techniques like risk assessment, security architecture, vulnerability assessment, forensic assessment, penetration testing etc.

Policy Exceptions

Despite the care that has been taken in authoring, reviewing and approving IS policy manual, there may be situations or circumstances which are not foreseen. It is conceivable that exceptional situations or emergencies occur and practical considerations clearly override or negate the policy statements made herein. Examples include the introduction of new legal or regulatory obligations that conflict with specific policy statements, or where following the policy to the letter and spirit would cause unacceptable health and safety risks.

In the event where someone identifies a situation in which this Policy cannot apply, it is their responsibility to raise the matter with the Director of MG. The Director, in conjunction with the

relevant IT assets Owner/s and other stakeholders, will take the decision on whether to permit or deny such policy exceptions depending on business justifications & risk mitigation controls.

Periodic Review

The policy shall be reviewed, every year or at the time of any major change in existing IT environment affecting policy and procedures. But the policy will be in force till its next review.

Policy Compliance Check

Policy plays a crucial role in the security architecture of assets of MG. So, there should be a periodic inspection towards the abidance/compliance of the policy across all the concerned.

IT Governance

The information technology structure is headed by the Director who reports to the Board of Directors.

Competent Authority

The Director will be deemed as Competent Authority for issues related to this policy unless explicitly mentioned otherwise.

3. Information Security Organization

3.1 Objective

Constantly evolving technology entails new threats and increased risks associated with automation. An organization level understanding of the responsibilities, threats and risks should be created to take adequate security measures, establish security organization and instil the security culture.

3.2 Scope

This policy applies to all users of IT Assets of MG including MG employees, employees of temporary employment agencies, vendor, business alliance partners, contractors/ sub-contractors and their personnel and functional units regardless of geographic location.

4. Third Party

4.1 Objective

The security of MG information processing facilities might be exposed to the risk of unauthorized access from External Parties users or outsourcing agencies, which needs to be adequately addressed and covered. Third Party includes Vendors, Contractor, Business Alliance Partners, Sub contractors and Customers etc.

4.2 Scope

This policy applies to all Third-Party personnel working in the MG's premises or from remote locations.

Third parties (vendors providing implementation/ continuation/ maintenance support) should be provided access to information Systems using hardware and software platforms and technologies approved by MG. The approval will be provided by the Director.

Third Party user's access to the banking client IT Systems should be restricted to the minimum services and functions necessary for the business functions performed by them. This includes both physical access and logical access to banking clients Information systems.

All third Parties having access to classified information should adhere to MG's IS Policy.The access should be granted to the third-party representatives as per the procedure on need to know basis subject to risk assessment and approval by competent authority.

Wherever possible, access to the 3rd party will be provided either through secure VPN Tunnel or by using a separate server with minimum data.

5. IT Assets Management

5.1 Objective

This section aims to ensure the clear identification & classification of IT assets, to provide traceability & appropriate protection to the IT assets.

5.2 SCOPE

This policy will apply to all the IT assets of MG.

5.3 IT Assets management

5.3.1 IT assets should be clearly identified. Each asset will have an owner who will be responsible for the asset. The IT assets should be properly labelled and classified.

5.3.2 Classifications

- Information Assets: This includes Databases and data files residing on various servers, PCs, Laptops, storage etc. including emails.
- Paper Assets: This includes files and documents in paper form (legal documents, contracts, user manuals and other files) including printouts and fax messages.
- Software Assets: This includes application, system software, software tools etc.

residing in the system or in storage media.

- Physical Assets: This includes servers, laptops, PCs, network devices, printers, removable media, storage etc.
- Services: This includes general support utilities like power, air conditioning, UPS, generators, software & hardware support (customization and maintenance) etc.
- People Assets: This includes people manning various operations of the above assets.

5.3.3 The Assets should be classified using the CIA attributes i.e.:

- Confidentiality
- Integrity
- Availability

5.3.4 Based on the above, the assets should be protected physically as well as logically with the most critical assets being given maximum protection.

5.4 Responsibility for maintaining/upgradation of IT assets

MG Director is responsible authority for maintenance / upgradation of critical IT assets systems & facilities.

6. Human Resource

6.1 Objective

Human Resource Security is to be implemented to address the risks of human error, lack of competence, theft, fraud or misuse of facilities and assist all personnel in creating a secure IT environment.

6.2 Scope

This policy applies to all MG employees who have been provided access to the IT Assets.

6.3 Human Resource Security

- The IT assets and functions should be handled by authorized staff.
- It should be ensured that the employees are trained appropriately.
- The security roles and responsibilities to be included in the job description.
- All employees to sign confidentiality & non-disclosure agreements.
- The segregation of duties to be defined so that no employee performs conflicting duties, wherever segregation of duties is not possible; there should be management control and oversight on the activities of the concerned employees.

7. Physical and Environment Security

7.1 Objective

The fundamental principles of Information Security, viz. Confidentiality, Integrity and Availability make it pertinent to encompass Physical & Environmental controls for the IT assets including Information processing facilities. The IT assets are secured from unauthorized access, damage, disruption, denial of access or interference and as such appropriate physical security measures are in place.

7.2 Scope

This policy covers within its scope all the information systems in use at all the locations.

7.3 Competent Authority

MG Director will be deemed as Competent Authority for issues related to Physical & Environmental Security.

7.4 Classification of areas in terms of usage and sensitivity:

- Server Area
- Support Services Area: This will constitute the support function areas like UPS/ Battery Room, Fire Fighting Equipment etc.
- Work Area: This will include the working space for the employees / external parties engaged in running the Information Processing Facilities.
- Storage Area: This will include the store room for spares, record room, file storage
- General function Area

7.5 Possible Treats to Physical and Environmental Security:

- Water seepage and floods
- Fire hazards
- Rodents
- Electrical malfunction
- Inflammable material

7.5.1 Possible Security measures (Indicative only):

- Adequate separation must be maintained between the server area and electrical installations.
- MG should provide fire detection and suppression; power conditioning, air conditioning and humidity controls and other environmental controls.
- All portable assets and removable media devices should be secured overnight under Lock & Key.

7.6 Security Inspections

- Periodic Security inspections of all sites and locations having Server Area and / or Support Service Area should be ensured.
- Security inspections of other sites are also desirable.

7.7 Monitoring and Logging

- The sensitive sites should have access to the authorized persons only and appropriate physical controls should be there i.e. locks etc.
- Any sensitive sites should be monitored by installing CCTVs & the CCTV footage should be monitored for any security breach.
- The logs of various access control devices like access cards, biometric access etc. should be reviewed and analysed.

8. Communication and Operations Management

8.1 Objective

This section aims to ensure the security of information processing methods, various business functions, and the protection of information across communication networks and technological infrastructures.

8.2 Scope

This policy covers within its scope all the information systems and the related business operations in use at the locations

8.3 Documentation of Operational Process

The IT operations should have standard operational procedures approved by the competent authority. These may be treated as formal documents and to be reviewed regularly and updated. The documentation be stored in a secure environment and protected from unauthorized access.

8.4 Change Management

Changes to information technology facilities and systems should be controlled in order to ensure that changes made to a production component are applied in a secure and consistent manner.

8.4.1 Change Management and Documentation

All changes should be scheduled and reviewed after the roll out. The change management process involves documenting and managing the change requests. Unscheduled/ Emergency changes should be carried out only in case there are critical production issues and not undertaken without proper notification to the controlling authority.

8.5 Patch & Service pack management

The patches released by the respective vendor should be identified & evaluated for applicability. Only tested versions of the patch or service pack should be considered for application, wherever needed. Role and Responsibility of IT Assets owners for updating patch should be in accordance with the policy.

8.6 Malicious Software

Users should be regularly made aware of the dangers of unauthorized or malicious software like computer viruses, network worms, Trojan horses and logic bombs.

8.7 Anti-Virus Management

The IT systems should have approved Anti-Virus Software with latest version installed and updated regularly.

8.8 Data Purging

It is to be ensured that preservation of purged data is to be done in synchronization with MG's guidelines on Record Maintenance Policy and is subjected to legal and regulatory requirements.

8.9 Business Contingency & Continuity Planning

- A Business Contingency & Continuity plan is a mechanism to anticipate stress situation emanating from all the four operational risks types i.e. People, Process, System & External Events and ensure continuation of operations under adverse conditions (i.e. interruption from natural or man-made hazards) without much loss of time.

8.10 Clock Synchronization

System clocks should be synchronized regularly especially between the various processing platforms.

9. Network Security Management Controls

9.1 Objective

This section aims to ensure the effectiveness, security and protection of information communication networks and technological infrastructures and also ensure secure, unencumbered flow of information across the network.

9.2 Scope

This policy covers within its scope the information systems in use at all the locations.

9.3 Network Security

The term 'Network' used in this policy section refers to all the types of networks like Local Area, Wide Area Network and Wireless Networks. The Internet and Intranet will be segregated and will not access each other.

9.4 Network Management Controls

Networks should be designed in conformance with reasonably secure practices. The design of the network is to be supported by formal documentation of the network details and users service requirements.

9.5 Network Services

The network services should be enabled only after assessing the security risks.

9.6 Wireless Network Security

Use of Wireless Network shall be restricted and reasonably secured based upon authorization from the competent authority.

9.6.1 Network Connectivity

Access to the network facilities is to be limited on the need to have principle & restricted to authorized persons only.

9.7 Network Devices

- **Routers/ Switches**

1. Routers/ Switches and consoles should be housed in a physically secure location.
2. Routers/ Switches should require a user to enter a user ID and Password to gain access to the command prompt.
3. Routers / Switches passwords are to be changed on a regular basis.
4. Copies of the router/switch configuration files should be restricted to authorized persons.
5. The IOS upgrades for routers should be evaluated for applicability and suitability.
6. The maintenance fixes must be applied on the routers during non-peak or off business-hour time
7. Latest configuration of all the routers/ switches should be backed up regularly.
8. The router/ switch audit logs to be reviewed regularly where applicable.

- **Firewalls**

1. The firewall design and architecture to be decided based on the security requirements of the internal network
2. Networks accessing the MG resources from the public network (Internet) are to be allowed only controlled access. The user will be authenticated at the web server level.

- **Intrusion Protection System (IPS)**

    1. The devices should be configured for monitoring network traffic and Preventing security attacks on the system including denial of usage, masquerading etc.
    2. The devices should be capable to generate different alerts based on the priority of attention needed from the administrator

- **Auditing & Logging:** The critical events including system events, access and operations should be logged. The audit logs should be protected from unauthorized access. The logs should be retained for appropriate period as per MG's Record Maintenance Policy taking into consideration the legal & regulatory requirements also.

- **Monitoring and Maintenance:** The critical servers should be monitored and maintained regularly. The activities of the administrators should also be monitored.

10. Data Backup Management

10.1 Objective

The objective is to ensure that all software & data are backed up regularly in order to ensure that it can be recovered in the event of systems failure, loss of service, loss/corruption of data or whenever required for meeting the business, legal & regulatory requirements.

10.2 Scope

This policy covers within its scope the information systems and the related business operations in use at all the locations.

10.3 Security Controls

- Audit logs on critical servers and devices should be enabled.
- Backup media movement should be controlled to avoid theft of Backup Media
- Backup media should be clearly and distinctly labelled.
- The retention period of the backup should be maintained as per the record maintenance policy of the Bank and also should be in compliance with the regulatory and legal requirements and directives.
- On expiry of the life of the media, the data should be transferred to other appropriate media and the old media shall be destroyed /degaussed to prevent any data leakage.
- The backup needs to be tested at least annually for availability/readability of data for restoration.
- One copy of backup storage media needs to be stored on site and another at off- site. The off-site location needs to be carefully chosen to ensure that it is located at a sufficient distance to be unaffected by any disaster at the original site.

10.4 Data Archival

- Archived data should be stored on such a platform and using such a technology that future alteration/ modification/ deletion of the data is not possible, once the data is archived.

11. User Management Control

11.1 Objective

User Management controls are to be implemented across and information is made available to authorized persons and for the authorized purposes only.

11.2 Scope

This policy covers within its scope all the information systems in use at all the locations.

11.3 User Categories

The users can be categorized as under:

1. System Administrators
2. Database Administrators
3. Security Administrators
4. Network Administrators

5. Auditors
6. Application Users

11.4 User Types

The user types are as under:

- MG Employees: These users fall under all the above categories as per their work profile.
- Third party: These users may normally undertake roles under any of above categories as per the MG's requirements.
- Customers: These are users with defined access to information resources in the software applications.
- The physical and logical access to the users is as defined in chapters on Third party and Logical Access Control.

12. Logical Access Control

12.1 Objective

- Logical access controls are to be implemented to ensure the confidentiality, integrity and availability of data across and information is made available to and used for authorized purposes only.

- Logical access to information systems should be controlled. Access control standards should be clearly defined and implemented.

12.2 Scope

This policy covers within its scope all the information systems in use at all the locations.

12.3 User Access Management

- User Access to Information, Data and Application: Users should be granted access to information, data and applications strictly on a 'need to know' and 'need to do' basis.

- Access Logs should be monitored and reviewed regularly.

- Managing User IDs: User IDs creation needs to follow a standard naming convention for IT assets to facilitate user identification and monitoring.

12.4 Password Management

Password Management and allocation should be in accordance with the password management & allocation guidelines.

User Authentication & Log On: Users accessing the system may be identified & authenticated using their credentials only before granting the access.

12.5 Logical Security on User Media

- Securing information on Laptops and Desktops: CD/DVD writers, USB Ports & Card Slotson end-user machines need to be disabled in order to prevent data theft / leakage. The same may be enabled for specific business requirement after getting approval from the competent authority.
- Security of Unattended User Media

1. The user to ensure not to leave any equipment unattended when logged in.
2. An appropriate locking mechanism e.g. a password protected screen saver may be used
3. The active sessions should be terminated, when not in use.
4. All paper & computer media-based IT assets need to be stored in suitable locked cabinets, when not in use, especially beyond working hours.
5. Important information, when printed, should be cleared from printer immediately.

12.6 Privilege Access management

Usage of privileged user IDs is restricted & controlled. Detailed Logical Access procedures will define the type of access, level of access and permissions for the servers, applications and databases.

12.7 Security of Alternate Delivery Channels

- MG should make mandatory disclosures of risks, responsibilities and liabilities of the customers in doing business through mobile phone/ Internet access.

12.8 Phishing, Vishing & Social Engineering

- Phishing: The fraudsters attempt to lure the customers into revealing their login credentials by sending fraudulent e-mails purporting to be from MG and asking the customers to reveal their passwords etc.

  The fraudsters may also create clone web pages similar to MG web site which may mislead the customer into thinking it to be MG's site.

- Vishing: Fraudsters may try to make customers reveal their credentials by contacting them over phone and misrepresenting as authorised officials of MG.

- Social Engineering: Fraudsters may attempt to lure the customers by use of social engineering to divulge sensitive information. Social engineers often rely on the natural helpfulness of people as well as on their weaknesses. It may include mails, telephonic calls, SMS, letters, personal contacts etc.

- MG has to create awareness among customers not to reply to the fraud emails, not to click on any link embedded in the email etc. Suitable disclaimers will be placed on MG's websites and in the printed form of security brochures, pin-mailers etc.

13. Information Systems Acquisition, Development and Maintenance

13.1 Objective

The security controls necessary in the process of Planning, Requirement analysis, Designing, Development, Implementation, processing of Data shall be defined, documented and implemented.

13.2 Scope

The policy is applicable to developed applications / software solution from outside developers such as Business Alliance Partners.

13.3 Controls Related to System Development Life Cycle

13.3.1 Planning and Initiation Phase: A risk analysis needs to be performed to determine the threats associated and the corresponding security controls required for the information system or system application under acquisition/ development / procurement.

13.3.2 Acquisition/ Development/ Procurement Phase

- While purchasing an information system or software, the security requirements should be specified in the Request for Proposal and the selection criteria shall be based on secure functionality
- Application controls are designed into all software applications to prevent loss, modification or misuse of user data. These controls may include:-

  - Use test environment to develop the software distinct from the production environment.
  - Validation of input data
  - Checks to detect inconsistent data
  - Control of internal processing
  - Limited Manual Intervention & Controls over any overrides
  - Validation of output data
  - A clear separation of access for UAT and production environments should be ensured. People having access to UAT environment should not have access to the production or vice- versa. In exceptional situation, wherein it is entirely necessary to give both the access to a specific person, complete logs should be available and checked for the activities done. After completion of activities, such access should be removed/ disabled.

13.3.3 Testing Phase: The modifications, enhancements and installation or implementation of new systems should be subject to 'Module Test', 'Integration Test' and 'Acceptance Test' by the appropriate users prior to installation into production.

13.3.4 Implementation Phase: Before the implementation of a new system, standard operating procedures including the security controls need to be prepared.

13.3.5 Operations / Maintenance Phase: The requisite procedures for operational tasks should be documented and updated regularly. Access to this system documentation shall be restricted. Access rights be reviewed periodically.

13.3.6 Restriction on Changes to Software Packages

- Wherever feasible, vendor supplied software packages should not be modified and if changes are essential then the original software shall be retained and the changes shall be applied to a clearly identified copy. While executing the changes, care should be taken to avoid the possibility of compromising the built in controls protection of log information.

13.3.7 Administrator and operator logs:

- Administration and operators logs should be reviewed regularly.

13.4 Application / Data migration

- Data/Application owner should ensure integrity and security during the entire process of migration.

13.5 Operating System Security

13.5.1 Security Controls

- Access to the Operating System need to be designed in a way that restricts access rights on need-to-do basis.

13.5.2 Restrictions on changes to software packages

- Any change would follow the defined Change Management procedure.

13.5.3 Administrator and operator logs

- Administrator and operator actions on all infrastructure & production systems/ Equipment should be logged and protected against change.

13.6 Database security

- A proper authentication mechanism should be put in place for granting access to the databases.
- Direct access to database should not be allowed. In case of requirements, Director would be the competent authority to provide exception on business justification.

13.7 Privacy of Information

- Any information collected and logged / captured by network devices and analytic tools is kept confidential. It is not disclosed to any other person. However, MG reserves the right to disclose the information to legal and regulatory authorities if required.

13.8 Application Security:

- The applications need to be developed by using a formal Software Development Life Cycle (SDLC).
- The security controls should be defined in the application at the design stage itself.
- Before moving into production, the application should be checked for vulnerability, weakness in coding and for existence of Trojans or backdoors using appropriate tools.
- All application systems need to have audit trails along with log monitoring capability. The logs generated should have distinct fields such as time stamp, user ID, activity performed etc.
- The audit trails need to be stored for a period as stipulated in the Record Maintenance Policy.

Web Server Security

All MG's Web pages, whether hosted on MG servers or external Web servers, need to be established, maintained and administered in a secure environment.

13.9.1 Controls for ensuring secure Web Server

- Web servers should be placed in DMZ (demilitarized zone) so that traffic between the Internet and the Web server is isolated from the internal network.
- The integrity of electronically published information should be secured against unauthorized modification. Proper authorization process is followed before any information is made publicly available.
- Minimum 128 bit SSL is used to secure browser to web server communication and also ensure server authentication.

13.9.2 Web Site Development Standard Necessary Disclaimer, Terms of Use and Privacy Policy should be placed on the home page of the Web sites and the regulatory guidelines should be followed.

13.10 Sharing of Information Assets.

Before sharing of MG's information assets with third parties & outside organization, risk assessment should be undertaken and appropriate controls should be put in place to ensure compliance to MG's Information Security policy.

13.11 Use of Authorized software

Only authorized and licensed software should be used in Bank. Freeware/ Shareware is to be used only after approval of the Director.

14. Incident Management

14.1 Objective

The term "Incident" in this document can be defined as any irregular or adverse event, which occurs on any part of MG information systems. Incident management is required to minimize the damage from security incidents.

14.2 Scope

This policy covers within its scope the information systems in use at all the locations.

14.3 Incident Management Coverage

- Incident management should include collection of information, its analysis apart

from recovering from the incident and avoidance of same in future.

- Incident management must cover different types of potential security incidents.

  Some examples are:-

  - Theft of / damage to computer hardware equipment and communication network
  - Theft/fire/property damage
  - Abusive usage of MG assets
  - Information system failures and loss of service
  - Illegal access to a system/ Breaches of confidentiality
  - Deliberate denial of service
  - Virus and Worm incidents
  - Errors resulting from incomplete or inaccurate business data
  - Errors resulting from inaccurate/ incomplete processing of data

- Awareness should be created amongst all employees, contractors and third party staff to report suspected security weaknesses quickly.

14.4 Incident Reporting

- Users should report incidents through designated channels.
- A record must be kept for all security incidents, which are under investigation.
- The procedure for collection and safeguarding of evidence should be defined and documented for purpose of disciplinary action within the organization as well as to ensure their admissibility in the court.

14.5 Learning from Incidents

- A follow-up analysis of the incident should be performed after an incident has been fully handled and all systems have been restored to a normal mode of operation to enable designing of controls to avoid further occurrence of the incident.
- A security incident report and Post Incident Report should be prepared.
- The information gained from the evaluation of information security incidents should be used to identify recurring or high impact incidents.

15. Internet Security

15.1 Objective

The purpose of this policy is to ensure that any internet access by MG's users is in a secure manner. It will help to protect information systems from attacks through the Internet.

15.2 Scope

This document addresses Policy related to Internet access. This Policy applies to the employees of MG and external parties who need access to Assets.

15.3 Access to Internet

MG provides Internet access on need to know basis. Access should be for an appropriate level duly approved from a competent authority. The Internet and Intranet will be segregated and will not access each other.

15.4 Authorized and Unauthorized use of Internet

Internet usage should be restricted to serve approved business requirements.

15.5 Web Site Blocking

Internal users should be blocked from accessing Web Sites that are deemed inappropriate. All the Web pages, whether hosted on MG or external Web servers, shouldbe created, maintained and administered in a secure environment.

16. E-Mail Security

16.1 Objective

The purpose of E-Mail Security policy is to ensure that electronic mail services are available when required by the authorized users of MG; the confidentiality and integrity of messages is protected in transit; and the risk of misuse is minimized.

16.2 Scope

This policy covers appropriate use of email sent through MG mail messaging system and applies to all staff and external parties operating on behalf of MG.

16.3 Email ID

- The Email ID creation/deletion should be undertaken after approval from the competent authority.
- The E-Mail facility should be used for Authorized purpose only and also as specified in the E mail Security Policy of the Bank.

16.4 Security Feature

- Users are prohibited from sending Restricted Information or data via e-mail.
- For sending business data, encryption and message authentication should be used.
- Bulk mailing should be available as a service only under exception.
- All Incoming / Outgoing Emails should be scanned for viruses and other malicious content
- User login and logouts should be logged, and Server Logs will be reviewed periodically, and relevant action will be taken based on the finding.
- All e-mails sent via should carry an automatic standard footer banner including an approved disclaimer.

17. Compliance

17.1 Objective

The objective for ensuring compliance is to avoid breaches of any criminal and civil law, and statutory, regulatory or contractual requirements. All the employees should be aware about legal aspects of using information systems and their responsibilities for ensuring compliance to the same. MG shall identify all the relevant acts and regulations applicable to its environment and make all employees aware about the same.

17.2 Scope

This policy applies to all staff, contracted personnel and representatives/officials of external parties who have been provided access to the IT assets of MG.

17.3 Legal Compliance

- Information Security Policy should comply with the legal and regulatory requirements
- A comprehensive listing of all relevant statutory, regulatory and contractual information security requirements should be maintained.
- Intellectual property rights should be classified appropriately for the Information IT assets.

18 Conclusion

As defined, the purpose of this policy is to provide a framework to ensure a secured IT environment for all the stakeholders i.e. MG, Staff, customers and all related 3rd parties. Based on this policy we have to devise specific and appropriate Processes/ Procedures/Controls for all the areas to ensure the implementation of this policy in Letter and Spirit.