Information Security Policy
Muslim Co-Operative Bank. Pvt . Ltd

Author:	
Owner:	Muslim Co-Operative Bank. Pvt. Ltd
Organization:	Muslim Co-Operative Bank. Pvt. Ltd
Document No:	Information Security Policy
Version No:	1.0
Date:	23rd April 2019

Document Control

Document Title Information Security Policy

Version History

Version No	Version Date	Author	Summary of Changes
1.0	09/10/2018		

Approvals

Name	Title	Date of Approval	Version No

Distribution

Name	Title	Date of Issue	Version No

Table of Contents

1 Introduction

1.1 Purpose

This policy defines the technical controls and security configurations users and Information Technology (IT) administrators are required to implement in order to ensure the integrity and availability of the data environment at Muslim Co-Operative Bank. Pvt. Ltd, hereinafter, referred to as the **Muslim Co-Operative Bank**. It serves as a central policy document with which all employees and contractors must be familiar and defines actions and prohibitions that all users must follow. The policy provides IT managers within the Muslim Co-Operative Bank with policies and guidelines concerning the acceptable use of Muslim Co-Operative Bank technology equipment, e-mail, Internet connections, voice-mail, facsimile, future technology resources and information processing.

The policy requirements and restrictions defined in this document shall apply to network infrastructures, databases, external media, encryption, hardcopy reports, films, slides, models, wireless, telecommunication, conversations, and any other methods used to convey knowledge and ideas across all hardware, software, and data transmission mechanisms. This policy must be adhered to by all Muslim Co-Operative Bank employees or temporary workers at all locations and by contractors working with the Muslim Co-Operative Bank as subcontractors.

1.2 Scope

This policy document defines common security requirements for all Muslim Co-Operative Bank personnel and systems that create, maintain, store, access, process or transmit information. This policy also applies to information resources owned by others, such as contractors of the Muslim Co-Operative Bank, entities in the private sector, in cases where Muslim Co-Operative Bank has a legal, contractual or fiduciary duty to protect said resources while in Muslim Co-Operative Bank custody. In the event of a conflict, the more restrictive measures apply. This policy covers the Muslim Co-Operative Bank network system which is comprised of various hardware, software, communication equipment and other devices designed to assist the Muslim Co-Operative Bank in the creation, receipt, storage, processing, and transmission of information. This definition includes equipment connected to any Muslim Co-Operative Bank domain or VLAN, either hardwired or wirelessly, and includes all stand-alone equipment that is deployed by the Muslim Co-Operative Bank at its office locations or at remote locales.

1.3 Acronyms / Definitions

Common terms and acronyms that may be used throughout this document.

CEO – The Chief Executive Officer is responsible for the overall privacy and security policy of the bank.

CIO – The Chief Information Officer

CMO – The Chief Medical Officer.

CO – The Confidentiality Officer is responsible for annual security training of all staff on confidentiality issues.

CPO – The Chief Security Officer is responsible for policy compromise issues.

CST – Confidentiality and Security Team

Encryption – The process of transforming information, using an algorithm, to make it unreadable to anyone other than those who have a specific 'need to know.'

External Media –i.e. CD-ROMs, DVDs, floppy disks, flash drives, USB keys, thumb drives and tapes

FAT – File Allocation Table - The FAT file system is relatively uncomplicated and an ideal format for floppy disks and solid-state memory cards. The most common implementations have a serious drawback in that when files are deleted and new files written to the media, their fragments tend to become scattered over the entire media, making reading and writing a slow process.

Firewall – a dedicated piece of hardware or software running on a computer which allows or denies traffic passing through it, based on a set of rules.

FTP – File Transfer Protocol

IT - Information Technology

LAN – Local Area Network – a computer network that covers a small geographic area, i.e. a group of buildings, an office.

NTFS – New Technology File Systems **–** NTFS has improved support for metadata and the use of advanced data structures to improve performance, reliability, and disk space utilization plus additional extensions such as security access control lists and file system journaling. The exact specification is a trade secret of Microsoft.

SOW - Statement of Work - An agreement between two or more parties that detail the working relationship between the parties and list a body of work to be completed.

User - Any person authorized to access an information resource.

Privileged Users – system administrators and others specifically identified and authorized by Muslim Co-Operative Bank management.

Users with edit/update capabilities – individuals, who are permitted, based on job assignment, to add, delete, or change records in a database**.**

Users with inquiry (read only) capabilities – individuals who are prevented, based on job assignment, from adding, deleting, or changing records in a database. Their system access is limited to reading information only.

VLAN – Virtual Local Area Network – A logical network, typically created within a network device, usually used to segment network traffic for administrative, performance and/or security purposes.

VPN – Virtual Private Network – Provides a secure passage through the public Internet.
WAN – Wide Area Network – A computer network that enables communication across a broad area, i.e. regional, national.
Virus - a software program capable of reproducing itself and usually capable of causing great harm to files or other programs on the computer it attacks. A true virus cannot spread to another computer without human assistance.

1.4 Applicable Statutes / Regulations

1.4.1 Indian IT Act 2008

Each of the policies defined in this document is applicable to the task being performed – not just to specific departments or job titles.

1.5 Security Officer

This Security Officer will oversee all ongoing activities related to the development, implementation, and maintenance of the Muslim Co-Operative Bank privacy policies in accordance with applicable Indian IT laws. The current Security Officer for the Muslim Co-Operative Bank is:

Name – Telephone Number[8]

1.6 Confidentiality / Security Team (CST)

The Muslim Co-Operative Bank has established a Confidentiality / Security Team made up of key personnel whose responsibility it is to identify areas of concern within the Muslim Co-Operative Bank and act as the first line of defence in enhancing the appropriate security posture.

All members identified within this policy are assigned to their positions by the CEO. The term of each member assigned is at the discretion of the CEO, but generally it is expected that the term will be one year. Members for each year will be assigned at the first meeting of the Muslim Co-Operative Bank in a new calendar year. This committee will consist of the positions within the Muslim Co-Operative Bank most responsible for the overall security policy planning of the organization- the CEO, PO, CMO, ISO, and the CIO (where applicable). The current members of the CST are:

Title – Name[9]
Title – Name
Title – Name
Title – Name

The CST will meet quarterly to discuss security issues and to review concerns that arose during the quarter. The CST will identify areas that should be addressed during annual training and review/update security policies as necessary.

The CST will address security issues as they arise and recommend and approve immediate security actions to be undertaken. It is the responsibility of the CST to identify areas of concern within the Muslim Co-Operative Bank and act as the first line of defence in enhancing the security posture of the Muslim Co-Operative Bank.

The CST is responsible for maintaining a log of security concerns or confidentiality issues. This log must be maintained on a routine basis, and must include the dates of an event, the actions taken to address the event, and recommendations for personnel actions, if appropriate. This log will be reviewed during the quarterly meetings.

The Security Officer (SO) or other assigned personnel is responsible for maintaining a log of security enhancements and features that have been implemented to further protect all sensitive information and assets held by the Muslim Co-Operative Bank. This log will also be reviewed during the quarterly meetings.

2 Employee Responsibilities

2.1 Employee Requirements

The first line of defense in data security is the individual Muslim Co-Operative Bank user. Muslim Co-Operative Bank users are responsible for the security of all data which may come to them in whatever format. The Muslim Co-Operative Bank is responsible for maintaining ongoing training programs to inform all users of these requirements.

Wear Identifying Badge so that it may be easily viewed by others -
In order to help maintain building security, all employees should prominently display their employee identification badge. Contractors who may be in Muslim Co-Operative Bank facilities are provided with different colored identification badges. Other people who may be within Muslim Co-Operative Bank facilities should be wearing visitor badges and should be chaperoned.

Challenge Unrecognized Personnel - It is the responsibility of all Muslim Co-Operative Bank personnel to take positive action to provide physical security. If you see an unrecognized person in a restricted Muslim Co-Operative Bank office location, you should challenge them as to their right to be there. All visitors to Muslim Co-Operative Bank offices must sign in at the front desk. In addition, all visitors, excluding patients, must wear a visitor/contractor badge. All other personnel must be employees of the Muslim Co-Operative Bank. Any challenged person who does not respond appropriately should be immediately reported to supervisory staff.

Secure Laptop with a Cable Lock - When out of the office all laptop computers must be secured with the use of a cable lock. Cable locks are provided with all new laptops computers during the original set up. All users will be instructed on their use and a simple user document, reviewed during employee orientation, is included on all laptop computers.

Most Muslim Co-Operative Bank computers will contain sensitive data either of organization details, personnel, or financial nature, and the utmost care should be taken to ensure that this data is not compromised. Laptop computers are unfortunately easy to steal, particularly during the stressful period while traveling. The cable locks are not fool proof but do provide an additional level of security. Many laptop computers are stolen in snatch and run robberies, where the thief runs through an office or hotel room and grabs all of the equipment, he/she can quickly remove. The use of a cable lock helps to thwart this type of event.

Unattended Computers - Unattended computers should be locked by the user when leaving the work area. This feature is discussed with all employees during yearly security training. Muslim Co-Operative Bank policy states that all computers will have the automatic screen lock function set to automatically activate upon 5(Five) minutes of

inactivity. Employees are not allowed to take any action which would override this setting.

Home Use of Muslim Co-Operative Bank Corporate Assets - Only computer hardware and software owned by and installed by the Muslim Co-Operative Bank is permitted to be connected to or installed on Muslim Co-Operative Bank equipment. Only software that has been approved for corporate use by the Muslim Co-Operative Bank may be installed on Muslim Co-Operative Bank equipment. Personal computers supplied by the Muslim Co-Operative Bank are to be used solely for business purposes. All employees and contractors must read and understand the list of prohibited activities that are outlined below. Modifications or configuration changes are not permitted on computers supplied by the Muslim Co-Operative Bank for home use.

Retention of Ownership - All software programs and documentation generated or provided by employees, consultants, or contractors for the benefit of the Muslim Co-Operative Bank are the property of the Muslim Co-Operative Bank unless covered by a contractual agreement. Nothing contained herein applies to software purchased by Muslim Co-Operative Bank employees at their own expense.

2.2 Prohibited Activities

Personnel are prohibited from the following activities. The list is not inclusive. Other prohibited activities are referenced elsewhere in this document.

- **Crashing an information system.** Deliberately crashing an information system is strictly prohibited. Users may not realize that they caused a system crash, but if it is shown that the crash occurred as a result of user action, a repetition of the action by that user may be viewed as a deliberate act.
- **Attempting to break into an information resource or to bypass a security feature.** This includes running password-cracking programs or sniffer programs, and attempting to circumvent file or other resource permissions.
- **Introducing, or attempting to introduce, computer viruses, Trojan horses, peer-to-peer ("P2P") or other malicious code into an information system.**

  Exception: Authorized information system support personnel, or others authorized by the Muslim Co-Operative Bank Security Officer, may test the resiliency of a system. Such personnel may test for susceptibility to hardware or software failure, security against hacker attacks, and system infection.
- **Browsing.** The willful, unauthorized access or inspection of confidential or sensitive information to which you have not been approved on a "need to know" basis is prohibited. The Muslim Co-Operative Bank has access to patient level health information which is protected by HIPAA regulations which stipulate a "need to know" before approval is granted to view the information. The purposeful attempt to look at or access information to which you have not been granted access by the appropriate approval procedure is strictly prohibited.

- **Personal or Unauthorized Software.** Use of personal software is prohibited. All software installed on Muslim Co-Operative Bank computers must be approved by the Muslim Co-Operative Bank.
- **Software Use.** Violating or attempting to violate the terms of use or license agreement of any software product used by the Muslim Co-Operative Bank is strictly prohibited.
- **System Use.** Engaging in any activity for any purpose that is illegal or contrary to the policies, procedures or business interests of the Muslim Co-Operative Bank is strictly prohibited.

2.3 Reporting Software Malfunctions

Users should inform the appropriate Muslim Co-Operative Bank personnel when the user's software does not appear to be functioning correctly. The malfunction - whether accidental or deliberate - may pose an information security risk. If the user, or the user's manager or supervisor, suspects a computer virus infection, the Muslim Co-Operative Bank computer virus policy should be followed, and these steps should be taken immediately:

- Stop using the computer
- Do not carry out any commands, including commands to <Save> data.
- Do not close any of the computer's windows or programs.
- Do not turn off the computer or peripheral devices.
- If possible, physically disconnect the computer from networks to which it is attached.
- Inform the appropriate personnel or Muslim Co-Operative Bank ISO as soon as possible. Write down any unusual behavior of the computer (screen messages, unexpected disk access, unusual responses to commands) and the time when they were first noticed.
- Write down any changes in hardware, software, or software use that preceded the malfunction.
- Do not attempt to remove a suspected virus!

The ISO should monitor the resolution of the malfunction or incident, and report to the CST the result of the action with recommendations on action steps to avert future similar occurrences.

2.4 Report Security Incidents

It is the responsibility of each Muslim Co-Operative Bank employee or contractor to report perceived security incidents on a continuous basis to the appropriate supervisor or security person. A User is any person authorized to access an information resource. Users are responsible for the day-to-day, hands-on security of that resource. Users are to formally report all security incidents or violations of the security policy immediately to the Security Officer Users should report any perceived security incident to either their immediate supervisor, or to their department head, or to any member of the Muslim Co-Operative Bank CST. Members of the CST are specified above in this document.

Reports of security incidents shall be escalated as quickly as possible. Each member of the Muslim Co-Operative Bank CST must inform the other members as rapidly as possible. Each incident will be analyzed to determine if changes in the existing security structure are necessary. All reported incidents are logged, and the remedial action indicated. It is the responsibility of the CST to provide training on any procedural changes that may be required as a result of the investigation of an incident.

Security breaches shall be promptly investigated. If criminal action is suspected, the Muslim Co-Operative Bank Security Officer shall contact the appropriate law enforcement and investigative authorities immediately, which may include but is not limited to the police or the FBI.

Transfer of Sensitive/Confidential Information

When confidential or sensitive information from one individual is received by another individual while conducting official business, the receiving individual shall maintain the confidentiality or sensitivity of the information in accordance with the conditions imposed by the providing individual. All employees must recognize the sensitive nature of data maintained by the Muslim Co-Operative Bank and hold all data in the strictest confidence. Any purposeful release of data to which an employee may have access is a violation of Muslim Co-Operative Bank policy and will result in personnel action and may result in legal action.

Transferring Software and Files between Home and Work

Personal software shall not be used on Muslim Co-Operative Bank computers or networks. If a need for specific software exists, submit a request to your supervisor or department head. Users shall not use Muslim Co-Operative Bank purchased software on home or on non-Muslim Co-Operative Bank computers or equipment.

Muslim Co-Operative Bank proprietary data, including but not limited to patient information, IT Systems information, financial information or human resource data, shall not be placed on any computer that is not the property of the Muslim Co-Operative Bank without written consent of the respective supervisor or department head. It is crucial to the Muslim Co-Operative Bank to protect all data and, in order to do that effectively we must control the systems in which it is contained. If a supervisor or department head receives a request to transfer Muslim Co-Operative Bank data to a non-Muslim Co-Operative Bank Computer System, the supervisor or department head should notify the Security Officer or appropriate personnel of the intentions and the need for such a transfer of data.

The Muslim Co-Operative Bank Wide Area Network (“WAN”) is maintained with a wide range of security protections in place, which include features such as virus protection, e-mail file type restrictions, firewalls, anti-hacking hardware and software, etc. Since the Muslim Co-Operative Bank does not control non-Muslim Co-Operative Bank personal computers, the Muslim Co-Operative Bank cannot be sure of the methods that may or may not be in place to protect Muslim Co-Operative Bank sensitive information, hence the need for this restriction.

Internet Considerations

Special precautions are required to block Internet (public) access to Muslim Co-Operative Bank information resources not intended for public access, and to protect confidential Muslim Co-Operative Bank information when it is to be transmitted over the Internet.

The following security and administration issues shall govern Internet usage.

Prior approval of the Muslim Co-Operative Bank Security Officer or appropriate personnel authorized by the Muslim Co-Operative Bank shall be obtained before:

- An Internet, or other external network connection, is established;
- Muslim Co-Operative Bank information (including notices, memoranda, documentation and software) is made available on any Internet-accessible computer (e.g. web or ftp server) or device;
- Users may not install or download any software (applications, screen savers, etc.). If users have a need for additional software, the user is to contact their supervisor;
- Use shall be consistent with the goals of the Muslim Co-Operative Bank. The network can be used to market services related to the Muslim Co-Operative Bank, however, use of the network for personal profit or gain is prohibited.
- Confidential or sensitive data - including credit card numbers, telephone calling card numbers, logon passwords, and other parameters that can be used to access goods or services - shall be encrypted before being transmitted through the Internet.
- The encryption software used, and the specific encryption keys (e.g. passwords, pass phrases), shall be escrowed with the Muslim Co-Operative Bank Security Officer or appropriate personnel, to ensure they are safely maintained/stored. The use of encryption software and keys, which have not been escrowed as prescribed above, is prohibited, and may make the user subject to disciplinary action.

Installation of authentication and encryption certificates on the e-mail system

Any user desiring to transfer secure e-mail with a specific identified external user may request to exchange public keys with the external user. Once verified, the certificate is installed on both recipients' workstations, and the two may safely exchange secure e-mail.

Use of WinZip encrypted and zipped e-mail

This software allows Muslim Co-Operative Bank personnel to exchange e-mail with remote users who have the appropriate encryption software on their system. The two users exchange private keys that will be used to both encrypt and decrypt each transmission. Any Muslim Co-Operative Bank staff member who desires to utilize this technology may request this software from the Security Officer or appropriate personnel.

De-identification / Re-identification of Personal Health Information (PHI)

As directed by HIPAA, all personal identifying information is removed from all data that falls within the definition of PHI before it is stored or exchanged.

De-identification is defined as the removal of any information that may be used to identify an individual or of relatives, employers, or household members.
PHI includes:

- Names
- Addresses
- Geographic subdivisions smaller than a state
- All elements of dates directly related to the individual (Dates of birth, marriage, death, etc)
- Telephone numbers
- Driver's license numbers
- Electronic mail addresses
- Aadhar No
- Bank Account numbers
- Biometric identifiers
- Full face photographic images and any comparable images

Re-identification of confidential information: A cross-reference code or other means of record identification is used to re-identify data if the code is not derived from or related to information about the individual and cannot be translated to identify the individual. In addition, the code is not disclosed for any other purpose nor is the mechanism for re-identification disclosed.

3 Identification and Authentication

3.1 User Logon IDs

Individual users shall have unique logon ids and passwords. An access control system shall identify each user and prevent unauthorized users from entering / using information resources. Security requirements for user identification include:

- Each user shall be assigned a unique identifier.
- Users shall be responsible for the use/misuse of their individual logon id.

All user login ids are audited at least twice yearly, and all inactive logon ids are revoked. The Muslim Co-Operative Bank HR department notifies the ISO upon the departure of all employees and contractors, at which time login ids are revoked.

The logon id is locked/revoked after a maximum of three (3) unsuccessful logon attempts which then require the passwords to be reset by the appropriate Administrator.

Users who desire to obtain access to Muslim Co-Operative Bank systems or networks must have a completed and signed Network Access Form (Appendix A). This form must be signed by the supervisor or department head of each user requesting access.

3.2 Passwords

User Account Passwords
User ids and passwords are required in order to gain access to all Muslim Co-Operative Bank networks and workstations. All passwords are restricted by a corporate wide password policy to be of a "Strong" nature. This means that all passwords must conform to restrictions and limitations that are designed to make the password difficult to guess. Users are required to select a password in order to obtain access to any electronic information both at the server level and at the workstation level. When passwords are reset, the user will be automatically prompted to manually change that assigned password.

Password Length – Passwords are required to be a minimum of eight characters.
Content Requirements - Passwords must contain a combination of upper- and lower-case alphabetic characters, numeric characters, and special characters.
Change Frequency – Passwords must be changed every 90 days. Compromised passwords shall be changed immediately.
Reuse - The previous three passwords cannot be reused.
Restrictions on Sharing Passwords - Passwords shall not be shared, or written down on paper, or stored within a file or database on a workstation and must be kept confidential.

Restrictions on Recording Passwords - Passwords are masked or suppressed on all online screens and are never printed or included in reports or logs. Passwords are stored in an encrypted format.

3.3 Confidentiality Agreement

Users of Muslim Co-Operative Bank information resources shall sign, as a condition for employment, an appropriate confidentiality agreement. The agreement shall include the following statement, or a paraphrase of it:

> *I understand that any unauthorized use or disclosure of information residing on the MUSLIM CO-OPERATIVE BANK information resource systems may result in disciplinary action consistent with the policies and procedures of federal, state, and local agencies.*

Temporary workers and third-party employees not already covered by a confidentiality agreement shall sign such a document prior to accessing Muslim Co-Operative Bank information resources.

Confidentiality agreements shall be reviewed when there are changes to contracts or other terms of employment, particularly when contracts are ending or employees are leaving an organization.

3.4 Access Control

Information resources are protected by the use of access control systems. Access control systems include both internal (passwords, encryption, access control lists, constrained user interfaces) and external (port protection devices, firewalls, host-based authentication).

Rules for access to resources (including internal and external telecommunications and networks) have been established by the information/application owner or manager responsible for the resources. Access is granted only by the completion of a Network Access Form. This form can only be initiated by the appropriate department head, and must be signed by the department head, and by the Security Officer or appropriate personnel.

Users may be added to the information system, network, or EHR **only** upon the signature of the Security Officer or appropriate personnel who is responsible for adding the employee to the network in a manner and fashion that ensures the employee is granted access to data only as specifically requested.

Online banner screens, if used, shall contain statements to the effect that unauthorized use of the system is prohibited, and that violators will be subject to criminal prosecution.

Identification and Authentication Requirements

The host security management program shall maintain current user application activity authorizations. Each initial request for a connection or a session is subject to the authorization process previously addressed.

4 IT Asset Management

4.1 IT Asset Management

The purpose of the IT Asset Management Policy is to maintain accurate records of the firm's physical computer assets. This document establishes procedures to ensure compliance with government regulations, legal industry standards and to ensure accurate reporting of physical assets.
This policy will apply to all computer equipment and related assets purchased by Muslim Co-Operative bank Safeguarding Responsibilities All items purchased will be recorded and maintained on a Fixed Asset Register by the IT Department. In order to manage the register accurately and efficiently, all employees shall adhere to the following;

1)Employees of Muslim Co-Operative bank shall not remove IT assets supplied by the firm from bank premises, except under the following conditions:

a. IT assets assigned to employees, which may include laptop or tablet computers and Personal Digital Assistant (PDA) or Smartphone devices, may be removed from for the following reasons only:

1.Teleworking.
2.Work that is outside of the office that is a part of an assigned position.

b. Exceptions to this policy must be requested in writing and approved by the Director of Information Security. Documentation of exceptions shall include the business or technical justification and the duration of the exception.

2) employees are responsible for safeguarding any IT assets they remove from the building, including keeping these assets under their direct physical control whenever possible, and physically securing the assets when they are not under the employee's direct physical control.

3) Muslim Co-Operative bank employees must immediately report the loss or theft of any assigned IT assets to the IT Department
4) Muslim Co-Operative bank employees are not allowed to bring their own IT assets into work locations with the purpose of connecting to the firm's private network and data.

a. In general, connection of personal IT assets to networks provided by the firm for guest or public access is not allowed.

b. Exceptions to this policy must be documented in writing and approved by the Director of Information Security. Documentation of exceptions shall include the business or technical justification and the duration of the exception.

4.2 Disposal of Assets

Disposal of firm assets, including the sale, transfer, donation, write off or sustainable disposal(recycling), must be done in adherence with all federal, state and local regulations. Computer hardware must have all software and information securely removed prior to disposal. Highly sensitive data must be deleted using secure methods as soon as they are no longer required. Secure methods of removal shall mean the use of software the can be configured to overwrite the data at least three times and or physical destruction of the hard drives to the extent that precludes any possible restoration of the da

5 Electronic Communication, E-mail, Internet Usage

5.1 Email Communication

As a productivity enhancement tool, The Muslim Co-Operative Bank encourages the business use of electronic communications. However, all electronic communication systems and all messages generated on or handled by Muslim Co-Operative Bank owned equipment are considered the property of the Muslim Co-Operative Bank – not the property of individual users. Consequently, this policy applies to all Muslim Co-Operative Bank employees and contractors, and covers all electronic communications including, but not limited to, telephones, e-mail, voice mail, instant messaging, Internet, fax, personal computers, and servers.

Muslim Co-Operative Bank provided resources, such as individual computer workstations or laptops, computer systems, networks, e-mail, and Internet software and services are intended for business purposes. However, incidental personal use is permissible if:

1) it does not consume more than a trivial amount of employee time or resources,
2) it does not interfere with staff productivity,
3) it does not preempt any business activity,
4) it does not violate any of the following:

    a) Copyright violations – This includes the act of pirating software, music, books and/or videos or the use of pirated software, music, books and/or videos and the illegal duplication and/or distribution of information and other intellectual property that is under copyright.
    b) Illegal activities – Use of Muslim Co-Operative Bank information resources for or in support of illegal purposes as defined by federal, state or local law is strictly prohibited.
    c) Commercial use – Use of Muslim Co-Operative Bank information resources for personal or commercial profit is strictly prohibited.
    d) Political Activities – All political activities are strictly prohibited on Muslim Co-Operative Bank premises. The Muslim Co-Operative Bank encourages all its employees to vote and to participate in the election process, but these activities must not be performed using Muslim Co-Operative Bank assets or resources.
    e) Harassment – The Muslim Co-Operative Bank strives to maintain a workplace free of harassment and that is sensitive to the diversity of its employees. Therefore, the Muslim Co-Operative Bank prohibits the use of computers, e-mail, voice mail, instant messaging, texting and the Internet in ways that are disruptive, offensive to others, or harmful to morale. For example, the display or transmission of sexually explicit images, messages, and cartoons is strictly prohibited. Other examples of misuse include, but is not limited to, ethnic slurs, racial comments, off-color jokes, or anything that may be

construed as harassing, discriminatory, derogatory, defamatory, threatening or showing disrespect for others.

f) Junk E-mail - All communications using IT resources shall be purposeful and appropriate. Distributing "junk" mail, such as chain letters, advertisements, or unauthorized solicitations is prohibited. A chain letter is defined as a letter sent to several persons with a request that each send copies of the letter to an equal number of persons. Advertisements offer services from someone else to you. Solicitations are when someone asks you for something. If you receive any of the above, delete the e-mail message immediately. Do not forward the e-mail message to anyone.

Generally, while it is **NOT** the policy of the Muslim Co-Operative Bank to monitor the content of any electronic communication, the Muslim Co-Operative Bank is responsible for servicing and protecting the Muslim Co-Operative Bank's equipment, networks, data, and resource availability and therefore may be required to access and/or monitor electronic communications from time to time. Several different methods are employed to accomplish these goals. For example, an audit or cost analysis may require reports that monitor phone numbers dialed, length of calls, number of calls to / from a specific handset, the time of day, etc. Other examples where electronic communications may be monitored include, but are not limited to, research and testing to optimize IT resources, troubleshooting technical problems and detecting patterns of abuse or illegal activity.

The Muslim Co-Operative Bank reserves the right, at its discretion, to review any employee's files or electronic communications to the extent necessary to ensure all electronic media and services are used in compliance with all applicable laws and regulations as well as Muslim Co-Operative Bank policies.

Employees should structure all electronic communication with recognition of the fact that the content could be monitored, and that any electronic communication could be forwarded, intercepted, printed or stored by others.

5.2 Internet Access

Internet access is provided for Muslim Co-Operative Bank users and is considered a great resource for the organization. This resource is costly to operate and maintain, and must be allocated primarily to those with business, administrative or contract needs. The Internet access provided by the Muslim Co-Operative Bank should not be used for entertainment, listening to music, viewing the sports highlight of the day, games, movies, etc. Do not use the Internet as a radio or to constantly monitor the weather or stock market results. While seemingly trivial to a single user, the bank wide use of these non-business sites consumes a huge amount of Internet bandwidth, which is therefore not available to responsible users.

Users must understand that individual Internet usage is monitored, and if an employee is found to be spending an excessive amount of time or consuming large amounts of bandwidth for personal use, disciplinary action will be taken.

Many Internet sites, such as games, peer-to-peer file sharing applications, chat rooms, and on-line music sharing applications, have already been blocked by the Muslim Co-Operative Bank routers and firewalls. This list is constantly monitored and updated as necessary. Any employee visiting pornographic sites will be disciplined and may be terminated.

6 Software Update

To ensure security and stability, it's critical to have standardized, well-documented practices for installing software updates. This policy offers guidelines for managing the update process, logging changes, and handling backups and device decommissioning.

From the policy: Maintaining a regular schedule of updates—as well as applying critical out-of-band patches as vulnerabilities are discovered—is paramount to maintaining the integrity of corporate security. With the advent of such threats as ransomware, performing regular security and platform updates, as well as creating backups if an update fails to install properly, is necessary to ensure that business operations can be conducted smoothly.

Update checking
There are two methods to determine whether updates are available or need to be performed.

Automatic checking

For Windows workstations and servers, preinstalled vendor-supplied software such as HP Support Assistant or Lenovo System Update automatically checks a database supplied by the vendor for updates to Intel ME or AMD PSP, system BIOS and firmware, and hardware drivers. Windows Update provides updates to the OS. Alternatively, Microsoft Update provides updates to Windows and other Microsoft software, including Office applications installed via the Microsoft Store that are updated through that interface. Other applications (such as Mozilla Firefox or Google Chrome) have their own internal update mechanism.

For network devices and workstations running Linux, these functions are handled in the package manager for your distribution. System BIOS updates may require manual patching.

Manual checking
Periodic checking of security bulletins relevant to the devices in use by the bank is necessary. Critical vulnerabilities that prompt vendors to issue out-of-band updates may necessitate emergency maintenance.

For Hardware Hardening Policy Please Refer: - Infrastructure Hardening Policy

7 Anti-virus, Software and Patch management

7.1 Antivirus Software Installation

Antivirus software is installed on all Muslim Co-Operative Bank personal computers and servers. Virus update patterns are updated daily on the Muslim Co-Operative Bank servers and workstations. Virus update engines and data files are monitored by appropriate administrative staff that is responsible for keeping all virus patterns up to date.

Configuration - The antivirus software currently implemented by the Muslim Co-Operative Bank is Seqrite End point security Antivirus. Updates are received directly from Seqrite End point security protection which is scheduled daily at 5:00 PM.

Monitoring/Reporting – A record of virus patterns for all workstations and servers on the Muslim Co-Operative Bank network may be maintained. Appropriate administrative staff is responsible for providing reports for auditing and emergency situations as requested by the Security Officer or appropriate personnel.

7.2 New Software Distribution

Only software created by Muslim Co-Operative Bank application staff, if applicable, or software approved by the Security Officer or appropriate personnel will be used on internal computers and networks. All new software will be tested by appropriate personnel in order to ensure compatibility with currently installed software and network configuration. In addition, appropriate personnel must scan all software for viruses before installation. This includes shrink-wrapped software procured directly from commercial sources as well as shareware and freeware obtained from electronic bulletin boards, the Internet, or on disks (magnetic or CD-ROM and custom-developed software).

Although shareware and freeware can often be useful sources of work-related programs, the use and/or acquisition of such software must be approved by the Security Officer or appropriate personnel. Because the software is often provided in an open distribution environment, special precautions must be taken before it is installed on Muslim Co-Operative Bank computers and networks. These precautions include determining that the software does not, because of faulty design, “misbehave” and interfere with or damage Muslim Co-Operative Bank hardware, software, or data, and that the software does not contain viruses, either originating with the software designer or acquired in the process of distribution.

All data and program files that have been electronically transmitted to a Muslim Co-Operative Bank computer or network from another location must be scanned for viruses immediately after being received. Contact the appropriate Muslim Co-Operative Bank personnel for instructions for scanning files for viruses.

Every diskette, CD-ROM, DVD and USB device are a potential source for a computer virus. Therefore, every diskette, CD-ROM, DVD and USB device must be scanned for virus infection prior to copying information to a Muslim Co-Operative Bank computer or network.

Computers shall never be “booted” from a diskette, CD-ROM, DVD or USB device received from an outside source. Users shall always remove any diskette, CD-ROM, DVD or USB device from the computer when not in use. This is to ensure that the diskette, CD-ROM, DVD or USB device is not in the computer when the machine is powered on. A diskette, CD-ROM, DVD or USB device infected with a boot virus may infect a computer in that manner, even if the diskette, CD_ROM, DVD or USB device is not “bootable”.

7.3 Retention of Ownership

All software programs and documentation generated or provided by employees, consultants, or contractors for the benefit of the Muslim Co-Operative Bank are the property of the Muslim Co-Operative Bank unless covered by a contractual agreement. Employees developing programs or documentation must sign a statement acknowledging Muslim Co-Operative Bank ownership at the time of employment. Nothing contained herein applies to software purchased by Muslim Co-Operative Bank employees at their own expense. **Title:**	**Physical Security**
Approval Date:	
Effective Date:	

8 Data Protection

8.1 Data Protection Policy

Muslim Co-Operative Bank needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact. This policy describes how this personal data must be collected, handled and stored to meet the bank's data protection standards

Data Backup: Backup procedures have been established that encrypt the data being moved to an external media. Use only that procedure – do not create one on your own. If there is not a backup procedure established or if you have external media that is not encrypted, contact the appropriate Muslim Co-Operative Bank personnel for assistance. Protect external media by keeping it in your possession when traveling.

Transferring Data to the Muslim Co-Operative Bank: Transferring of data to the Muslim Co-Operative Bank requires the use of an approved VPN connection to ensure the confidentiality and integrity of the data being transmitted. Do not circumvent established procedures, nor create your own method, when transferring data to the Muslim Co-Operative Bank.

External System Access: If you require access to an external system, contact your supervisor or department head. Security Officer or appropriate personnel will assist in establishing a secure method of access to the external system.

E-mail: Do not send any individual-identifiable information via e-mail unless it is encrypted. If you need assistance with this, contact the Security Officer or appropriate personnel to ensure an approved encryption mechanism is used for transmission through e-mail.

Non-Muslim Co-Operative Bank Networks: Extreme care must be taken when connecting Muslim Co-Operative Bank equipment to a home or hotel network. Although the Muslim Co-Operative Bank actively monitors its security status and maintains organization wide protection policies to protect the data within all contracts, the Muslim Co-Operative Bank has no ability to monitor or control the security procedures on non-Muslim Co-Operative Bank networks.

Protect Data in Your Possession: View or access only the information that you have a need to see to complete your work assignment. Regularly review the data you have stored to ensure that the amount of patient level data is kept at a minimum and that old data is eliminated as soon as possible.

Hard Copy Reports or Work Papers: Never leave paper records around your work area. Lock all paper records in a file cabinet at night or when you leave your work area.

Data Entry When in a Public Location: Do not perform work tasks which require the use of sensitive corporate or patient level information when you are in a public area, i.e. airports, airplanes, hotel lobbies. Computer screens can easily be viewed from beside or behind you.

Sending Data Outside the Muslim Co-Operative Bank: Do not give or transfer any patient level information to anyone outside the Muslim Co-Operative Bank without the written approval of your supervisor.

8.2 Retention / Destruction Data

The Muslim Co-Operative Bank actively conforms to these laws and follows the strictest regulation if/when a conflict occurs.

Record Retention - Documents relating to uses and disclosures, authorization forms, business partner contracts, notices of information Muslim Co-Operative Bank, and a complaint record are maintained for a period of 6 year.

Record Destruction - All hardcopy records that require destruction are shredded.

8.3 Disposal of Paper and/or External Media

Shredding: All paper which contains sensitive information that is no longer needed must be shredded before being disposed. Do not place in a trash container without first shredding. All employees working from home, or other non-Muslim Co-Operative Bank work environment, MUST have direct access to a shredder.

Disposal of Electronic Media:

- Do not throw any media containing sensitive, protected information in the trash.
- Return all external media to your supervisor

External media must be wiped clean of all data. The Security Officer or appropriate personnel has very definitive procedures for doing this – so all external media must be sent to them.

9 Network Connectivity

9.1 Dial-In Connections

Access to Muslim Co-Operative Bank information resources through modems or other dial-in devices / software, if available, shall be subject to authorization and authentication by an access control system. **Direct inward dialing without passing through the access control system is prohibited.**

Dial-up numbers shall be unlisted.

Systems that allow public access to host computers, including mission-critical servers, warrant additional security at the operating system and application levels. Such systems shall have the capability to monitor activity levels to ensure that public usage does not unacceptably degrade system responsiveness.

Dial-up access privileges are granted only upon the request of a department head with the submission of the Network Access Form and the approval of the Security Officer or appropriate personnel.

9.2 Dial Out Connections

Muslim Co-Operative Bank provides a link to an Internet Service Provider**.** If a user has a specific need to link with an outside computer or network through a direct link, approval must be obtained from the Security Officer or appropriate personnel. The appropriate personnel will ensure adequate security measures are in place

9.3 Telecommunication Equipment

Certain direct link connections may require a dedicated or leased phone line. These facilities are authorized only by the Security Officer or appropriate personnel and ordered by the appropriate personnel. Telecommunication equipment and services include but are not limited to the following:

- phone lines
- fax lines
- calling cards
- phone head sets
- software type phones installed on workstations
- conference calling contracts
- cell phones
- Blackberry type devices

- call routing software
- call reporting software
- phone system administration equipment
- T1/Network lines
- long distance lines
- 800 lines
- local phone lines
- PRI circuits
- telephone equipment

9.4 Permanent Connections

The security of Muslim Co-Operative Bank systems can be jeopardized from third party locations if security policy and resources are inadequate. When there is a need to connect to a third-party location, a risk analysis should be conducted. The risk analysis should consider the type of access required, the value of the information, the security measures employed by the third party, and the implications for the security of Muslim Co-Operative Bank systems. The Security Officer or appropriate personnel should be involved in the process, design and approval.

9.5 Emphasis on Security in Third Party Contracts

Access to Muslim Co-Operative Bank computer systems or corporate networks should not be granted until a review of the following concerns has been made, and appropriate restrictions or covenants included in a statement of work ("SOW") with the party requesting access.

- Applicable sections of the Muslim Co-Operative Bank Information Security Policy have been reviewed and considered.
- Policies and standards established in the Muslim Co-Operative Bank information security program have been enforced.
- A risk assessment of the additional liabilities that will attach to each of the parties to the agreement.
- The right to audit contractual responsibilities should be included in the agreement or SOW.
- Arrangements for reporting and investigating security incidents must be included in the agreement in order to meet the covenants of the HIPAA Business Associate Agreement.
- A description of each service to be made available.
- Each service, access, account, and/or permission made available should only be the minimum necessary for the third party to perform their contractual obligations.
- A detailed list of users that have access to Muslim Co-Operative Bank computer systems must be maintained and auditable.

- If required under the contract, permission should be sought to screen authorized users.
- Dates and times when the service is to be available should be agreed upon in advance.
- Procedures regarding protection of information resources should be agreed upon in advance and a method of audit and enforcement implemented and approved by both parties.
- The right to monitor and revoke user activity should be included in each agreement.
- Language on restrictions on copying and disclosing information should be included in all agreements.
- Responsibilities regarding hardware and software installation and maintenance should be understood and agreement upon in advance.
- Measures to ensure the return or destruction of programs and information at the end of the contract should be written into the agreement.
- If physical protection measures are necessary because of contract stipulations, these should be included in the agreement.
- A formal method to grant and authorized users who will access to the data collected under the agreement should be formally established before any users are granted access.
- Mechanisms should be in place to ensure that security measures are being followed by all parties to the agreement.
- A detailed list of the security measures which will be undertaken by all parties to the agreement should be published in advance of the agreement.

9.6 Firewalls

Authority from the Security Officer or appropriate personnel must be received before any employee or contractor is granted access to a Muslim Co-Operative Bank router or firewall.

10 Removable Media

10.1 Use of External Media

Transportable media included within the scope of this policy includes, but is not limited to, SD cards, DVDs, CD-ROMs, and USB key devices.

The purpose of this policy is to guide employees/contractors of the Muslim Co-Operative Bank in the proper use of transportable media when a legitimate business requirement exists to transfer data to and from Muslim Co-Operative Bank networks. Every workstation or server that has been used by either Muslim Co-Operative Bank employees or contractors is presumed to have sensitive information stored on its hard drive. Therefore procedures must be carefully followed when copying data to or from transportable media to protect sensitive Muslim Co-Operative Bank data. Since transportable media, by their very design are easily lost, care and protection of these devices must be addressed. Since it is very likely that transportable media will be provided to a Muslim Co-Operative Bank employee by an external source for the exchange of information, it is necessary that all employees have guidance in the appropriate use of media from other companies.

The use of transportable media in various formats is common Muslim Co-Operative Bank within the Muslim Co-Operative Bank. All users must be aware that sensitive data could potentially be lost or compromised when moved outside of Muslim Co-Operative Bank networks. Transportable media received from an external source could potentially pose a threat to Muslim Co-Operative Bank networks. ***Sensitive data*** includes all human resource data, financial data, Muslim Co-Operative Bank proprietary information.

Pen Drives are handy devices which allow the transfer of data in an easy to carry format. They provide a much improved format for data transfer when compared to previous media formats, like diskettes, CD-ROMs, or DVDs. The software drivers necessary to utilize a Pen Drives are normally included within the device and install automatically when connected. They now come in a rugged titanium format which connects to any key ring. These factors make them easy to use and to carry, but unfortunately easy to lose.

Rules governing the use of transportable media include:

- No ***sensitive data*** should ever be stored on transportable media unless the data is maintained in an encrypted format.
- All Pen Drives used to store Muslim Co-Operative Bank data or sensitive data must be an encrypted Pen Drives issued by the Security Officer or appropriate personnel. The use of a personal Pen Drives is strictly prohibited.
- Users must never connect their transportable media to a workstation that is not issued by the Muslim Co-Operative Bank.

- Non-Muslim Co-Operative Bank workstations and laptops may not have the same security protection standards required by the Muslim Co-Operative Bank, and accordingly virus patterns could potentially be transferred from the non-Muslim Co-Operative Bank device to the media and then back to the Muslim Co-Operative Bank workstation.

  Example: Do not copy a work spreadsheet to your Pen Drives and take it home to work on your home PC.

- Data may be exchanged between Muslim Co-Operative Bank workstations/networks and workstations used within the Muslim Co-Operative Bank. The very nature of data exchange requires that under certain situations data be exchanged in this manner.

  Examples of necessary data exchange include:
  Data provided to auditors via Pen Drives during the course of the audit.

- It is permissible to connect transferable media from other businesses or individuals into Muslim Co-Operative Bank workstations or servers as long as the source of the media in on the Muslim Co-Operative Bank Approved Vendor list (Appendix D).

- Before initial use and before any ***sensitive data*** may be transferred to transportable media, the media must be sent to the Security Officer or appropriate personnel to ensure appropriate and approved encryption is used. Copy ***sensitive data*** only to the encrypted space on the media. Non-sensitive data may be transferred to the non-encrypted space on the media.

- Report all loss of transportable media to your supervisor or department head. It is important that the CST team is notified either directly from the employee or contractor or by the supervisor or department head immediately.

- When an employee leaves the Muslim Co-Operative Bank, all transportable media in their possession must be returned to the Security Officer or appropriate personnel for data erasure that conforms to US Department of Defense standards for data elimination.

The Muslim Co-Operative Bank utilizes an approved method of encrypted data to ensure that all data is converted to a format that cannot be decrypted. The Security Officer or appropriate personnel can quickly establish an encrypted partition on your transportable media.

When no longer in productive use, all Muslim Co-Operative Bank laptops, workstation, or servers must be wiped of data in a manner which conforms to HIPAA regulations. All

transportable media must be wiped according to the same standards. Thus all transportable media must be returned to the Security Officer or appropriate personnel for data erasure when no longer in use.

10.2 Disposal of External Media

It must be assumed that any external media in the possession of an employee is likely to contain sensitive information. Accordingly, external media (CD-ROMs, DVDs, diskettes, USB drives) should be disposed of in a method that ensures that there will be no loss of data and that the confidentiality and security of that data will not be compromised.

The following steps must be adhered to:

- It is the responsibility of each employee to identify media which should be shredded and to utilize this policy in its destruction.
- External media should never be thrown in the trash.
- When no longer needed all forms of external media are to be sent to the Security Officer or appropriate personnel for proper disposal.

11 Physical Security

It is the policy of the Muslim Co-Operative Bank to provide building access in a secure manner. Each site, if applicable, is somewhat unique in terms of building ownership, lease contracts, entranceway access, fire escape requirements, and server room control. However, the Muslim Co-Operative Bank strives to continuously upgrade and expand its security and to enhance protection of its assets and medical information that has been entrusted to it. The following list identifies measures that are in effect at the Muslim Co-Operative Bank. All other facilities, if applicable, have similar security appropriate for that location.

647, Bhawani Peth, 4th Floor,
Golden Jubilee Technical Institute Building,
Pune - 411 042.

- Entrance to the office premises working hours is controlled by a biometric Attempted entrance without this biometric verification results in immediate notification to the police department.
- Biometric System stores biometric data of Muslim Co-Operative Bank employees or authorised personals only.
- Any unrecognized person in a restricted office location should be challenged as to their right to be there. All visitors must sign in at the front desk, wear a visitor badge (excluding patients), and be accompanied by a Muslim Co-Operative Bank staff member. In some situations, non-Muslim Co-Operative Bank personnel, who have signed the confidentiality agreement, do always not need to be accompanied. The building is equipped with security cameras to record activities in the parking lot and within the area encompassing the front entrance. All activities in these areas are recorded on a 24 hour a day 365 day per year basis.

12 Sanction Policy

It is the policy of the Muslim Co-Operative Bank that all workforce members must protect the confidentiality, integrity, and availability of sensitive information at all times. The Muslim Co-Operative Bank will impose sanctions, as described below, on any individual who accesses, uses, or discloses sensitive information without proper authorization.
The Muslim Co-Operative Bank will take appropriate disciplinary action against employees, contractors, or any individuals who violate the Muslim Co-Operative Bank's information security and privacy policies or *Information Technology Act*, 2000

To ensure that there are appropriate sanctions that will be applied to workforce members who violate the Muslim Co-Operative Bank's security policies, Directives, and/or any other Indian Government regulatory requirements.

Workforce member means employees, volunteers, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity. This includes full and part time employees, affiliates, associates, volunteers, and staff from third party entities who provide service to the covered entity.
Sensitive information, includes, but not limited to, the following:

- Personnel files – Any information related to the hiring and/or employment of any individual who is or was employed by the Muslim Co-Operative Bank.
- Payroll data – Any information related to the compensation of an individual during that individuals' employment with the Muslim Co-Operative Bank.
- Financial/accounting records – Any records related to the accounting Muslim Co-Operative Banks or financial statements of the Muslim Co-Operative Bank.
- Other information that is confidential – Any other information that is sensitive in nature or considered to be confidential.

Availability refers to data or information is accessible and useable upon demand by an authorized person.
Confidentiality refers to data or information is not made available or disclosed to unauthorized persons or processes.
Integrity refers to data or information that have not been altered or destroyed in an unauthorized manner.

Violations

Listed below are the types of violations that require sanctions to be applied. They are stated at levels 1, 2, and 3 depending on the seriousness of the violation.

Level	Description of Violation
1	• Accessing information that you do not need to know to do your job. • Sharing computer access codes (user name &

	password). • Leaving computer unattended while being able to access sensitive information. • Disclosing sensitive information with unauthorized persons. • Copying sensitive information without authorization. • Changing sensitive information without authorization. • Discussing sensitive information in a public area or in an area where the public could overhear the conversation. • Discussing sensitive information with an unauthorized person. • Failing/refusing to cooperate with the Information Security Officer, Privacy Officer, Chief Information Officer, and/or authorized designee.
2	• Second occurrence of any Level 1 offense (does not have to be the same offense). • Unauthorized use or disclosure of sensitive information. • Using another person's computer access code (user name & password). • Failing/refusing to comply with a remediation resolution or recommendation.
3	• Third occurrence of any Level 1 offense (does not have to be the same offense). • Second occurrence of any Level 2 offense (does not have to be the same offense). • Obtaining sensitive information under false pretenses. • Using and/or disclosing sensitive information for commercial advantage, personal gain, or malicious harm.

Recommended Disciplinary Actions

If a workforce member violates the Muslim Co-Operative Bank's privacy and security policies and/or violates the *Information Technology Act*, 2000, governing the protection of sensitive and patient identifiable information, the following recommended disciplinary actions will apply.

Violation Level	Recommended Disciplinary Action
1	• Verbal or written reprimand • Retraining on privacy/security awareness • Retraining on the Muslim Co-Operative Bank's privacy and security policies

	• Retraining on the proper use of internal or required forms
2	• Letter of Reprimand*; or suspension • Retraining on privacy/security awareness • Retraining on the Muslim Co-Operative Bank's privacy and security policies • Retraining on the proper use of internal or required forms
3	• Termination of employment or contract • Criminal penalties as provided under Information Technology Act, 2000

Important Note: The recommended disciplinary actions are identified in order to provide guidance in policy enforcement and are not meant to be all-inclusive. If formal discipline is deemed necessary, the Muslim Co-Operative Bank shall consult with Human Resources prior to taking action. When appropriate, progressive disciplinary action steps shall be followed allowing the employee to correct the behavior which caused the disciplinary action.

*A Letter of Reprimand must be reviewed by Human Resources before given to the employee.

Exceptions
Depending on the severity of the violation, any single act may result in disciplinary action up to and including termination of employment or contract with the Muslim Co-Operative Bank.

Acknowledgment

I, the undersigned employee or contractor, hereby acknowledges receipt of a copy of the Sanction Policy for Muslim Co-Operative Bank.

Dated this _____ day of _____, 20____.

_____
Signature of Employee/Contractor

13 Breach Notification Procedures

To outline the process for notifying affected individuals of a breach of protected information breach notification purposes.

This applies to all employees, volunteers, and other individuals working under contractual agreements with the Muslim Co-Operative Bank.

Personal Information – Personal Information has many definitions including definitions by statute which may vary from state to state. Most generally, Personal Information is a combination of data elements which could uniquely identify an individual. Please review applicable state data breach statutes to determine what definition of Personal Information is applicable for purposes of the document.

Personally Identifiable Information (PII) – Information in any form that consists of a combination of an individual's name and one or more of the following: Aadhar No, Pan No, Bank account numbers, credit card numbers, debit card numbers, personal code, security code, password, personal ID number, photograph, fingerprint, or other information which could be used to identify an individual.

Privacy Act Breach – Unauthorized acquisition or reasonable belief of unauthorized acquisition of personal information protected by the Privacy Act. This information includes, but is not limited to Aadhar No, Pan No, Bank account numbers, or other information posing a risk of identity theft.

Private Information – Information protected by the Privacy Act, Personally Identifiable Information, Personal Information.

Procedure

Reporting a Possible Breach

1. Any employee who becomes aware of a possible breach of privacy involving Private Information in the custody or control of the Muslim Co-Operative Bank will immediately inform their supervisor/manager, and the Privacy Officer.
2. Notification should occur immediately upon discovery of a possible breach or before the end of your shift if other duties interfere, however, in no case should notification occur later than twenty-four (24) hours after discovery.
    a. The supervisor/manager will verify the circumstances of the possible breach and inform the Security Officer and the division Administrator/Director within twenty-four (24) hours of the initial report.
3. You may call the Security Officer directly at _____-_____[32].
    a. Provide the Security Officer with as much detail as possible.
    b. Be responsive to requests for additional information from the Privacy Officer.
    c. Be aware that the Security Officer has an obligation to follow up on any reasonable belief that Private Information has been compromised.

4. The Security Officer, in conjunction with the Muslim Co-Operative Bank's Legal Counsel, will decide whether or not to notify the President/CEO as appropriate by taking into consideration the seriousness and scope of the breach.

Containing the Breach

1. The Security Officer will take the following steps to limit the scope and effect of the breach.
    a. Work with department(s) to immediately contain the breach. Examples include, but are not limited to:
        i. Stopping the unauthorized policy
        ii. Recovering the records, if possible
        iii. Shutting down the system that was breached
        iv. Mitigating the breach, if possible
        v. Correcting weaknesses in security policies
        vi. Notifying the appropriate authorities including the local Police Department if the breach involves, or may involve, any criminal activity

Investigating and Evaluating the Risks Associated with the Breach

1. To determine what other steps are immediately necessary, the Security Officer in collaboration with the Muslim Co-Operative Bank's Legal Counsel and affected department(s) and administration, will investigate the circumstances of the breach.
    a. A team will review the results of the investigation to determine root cause(es), evaluate risks, and develop a resolution plan.
        i. The Privacy Breach Assessment tool will help aid the investigation.
    b. The Security Officer, in collaboration with the Muslim Co-Operative Bank's Legal Counsel, will consider several factors in determining whether to notify individuals affected by the breach including, but not limited to:
        i. Contractual obligations
        ii. Legal obligations – the Muslim Co-Operative Bank's Legal Counsel should complete a separate legal assessment of the potential breach and provide the results of the assessment to the Security Officer and the rest of the breach response team
        iii. Risk of identity theft or fraud because of the type of information lost such as social security number, banking information, identification numbers
        iv. Risk of physical harm if the loss puts an individual at risk of stalking or harassment
        v. Risk of hurt, humiliation, or damage to reputation when the information includes medical or disciplinary records
        vi. Number of individuals affected

Notification

1. The Security Officer will work with the department(s) involved, the Muslim Co-Operative Bank's Legal Counsel and appropriate leadership to decide the best approach for notification and to determine what may be required by law.

2. If required by law, notification of individuals affected by the breach will occur as soon as possible following the breach.
    a. Affected individuals must be notified without reasonable delay, but in no case later than sixty (60) calendar days after discovery, unless instructed otherwise by law enforcement or other applicable state or local laws.
        i. Notices must be in plain language and include basic information, including:
            1. What happened
            2. Types of PHI involved
            3. Steps individuals should take
            4. Steps covered entity is taking
            5. Contact Information
        ii. Notices should be sent by first-class mail or if individual agrees electronic mail. If insufficient or out-of-date contact information is available, then a substitute notice is required as specified below.
    b. If law enforcement authorities have been contacted, those authorities will assist in determining whether notification may be delayed in order not to impede a criminal investigation.
3. The required elements of notification vary depending on the type of breach and which law is implicated. As a result, the Muslim Co-Operative Bank's Security Officer and Legal Counsel should work closely to draft any notification that is distributed.
4. Indirect notification such as website information, posted notices, media will generally occur only where direct notification could cause further harm, or contact information is lacking.
    a. If a breach affects five-hundred (500) or more individuals, or contact information is insufficient, the Muslim Co-Operative Bank will notify a prominent media outlet that is appropriate for the size of the location with affected individuals, and notice will be provided in the form of a press release.
5. Using multiple methods of notification in certain cases may be the most effective approach.

Business associates must notify the Muslim Co-Operative Bank if they incur or discover a breach of unsecured PHI.

1. Notices must be provided without reasonable delay and in no case later than sixty (60) days after discovery of the breach.
2. Business associates must cooperate with the Muslim Co-Operative Bank in investigating and mitigating the breach.

Notice to Health and Human Services (HHS) as required by HIPAA – If the Muslim Co-Operative Bank's Legal Counsel determines that HIPAA notification is not required; this notice is also not required.

1. Information regarding breaches involving five-hundred (500) or more individuals, regardless of location, must be submitted to HHS at the same time that notices to individuals are issued.

2. If a breach involves fewer than five-hundred (500) individuals, the Muslim Co-Operative Bank will be required to keep track of all breaches and to notify HHS within sixty (60) days after the end of the calendar year.

Prevention

1. Once immediate steps are taken to mitigate the risks associated with the breach, the Security Officer will investigate the cause of the breach.
    a. If necessary, this will include a security audit of physical, organizational, and technological measures.
    b. This may also include a review of any mitigating steps taken.
2. The Security Officer will assist the responsible department to put into effect adequate safeguards against further breaches.
3. Procedures will be reviewed and updated to reflect the lessons learned from the investigation and regularly thereafter.
4. The resulting plan will also include audit recommendations, if appropriate.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing these procedures. Employees who violate these procedures are subject to discipline up to and including termination in accordance with the Muslim Co-Operative Bank's Sanction Policy.

14 Appendix A – Network Access Request Form

Employee or Contractor Request for Network Access

EMPLOYEE/CONTRACTOR INFORMATION		
☐ New Employee ☐ New Contractor ☐ Existing User		Today's Date:
☐ Temporary		
First Name:	Last Name:	*MI:
Position:	Department: Supervisor:	
☐ Full-time ☐ Part-time	Start date or Requested due date: Temporary or Contractor end date, if known:	

SECURITY & EMAIL

New Account:
☐ Network Account ☐ Email
☐ Security/Email similar to what existing user:

☐ Include in which E-mail Group(s): ☐ Remove from which E-mail Group(s):

☐ Include in which Security Group(s): ☐ Remove from which Security Group(s):

☐ Permit access to the following network location(s):
Drive Path Access: ☐ Read-only ☐ Read/write ☐ Full Access ☐ Remove Access
Drive Path Access: ☐ Read-only ☐ Read/write ☐ Full Access ☐ Remove Access
Drive Path Access: ☐ Read-only ☐ Read/write ☐ Full Access ☐ Remove Access

☐ Miscellaneous Needs *(Enter any other requests)*:

EHR ACCESS

☐ EHR Account

Roles & Access:
☐ Front Office Access: ☐ Read-only ☐ Read/write ☐ Full Access ☐ Remove Access
☐ Clinician Access: ☐ Read-only ☐ Read/write ☐ Full Access ☐ Remove Access
☐ Physician Access: ☐ Read-only ☐ Read/write ☐ Full Access ☐ Remove Access
☐ Accounting Access: ☐ Read-only ☐ Read/write ☐ Full Access ☐ Remove Access

☐ Records Management Access: ☐ Read-only ☐ Read/write ☐ Full Access ☐ Remove Access
☐ Reporting Access: ☐ Read-only ☐ Read/write ☐ Full Access ☐ Remove Access
☐ Administrator Access: ☐ Read-only ☐ Read/write ☐ Full Access ☐ Remove Access
☐ Other: Specify Access: ☐ Read-only ☐ Read/write ☐ Full Access ☐ Remove Access

☐ Miscellaneous Needs *(Enter any other requests)*:

HARDWARE & SOFTWARE

Hardware:
☐ Laptop ☐ Desktop ☐ Either Laptop or Desktop
☐ Screen protector ☐ Laptop bag ☐ Cable lock
☐ Multifunction printer ☐ Netgear Router ☐ Numeric keypad
☐ Standard inkjet printer ☐ Dual monitors ☐ Docking station
☐ iPhone ☐ iPad ☐ Windows Mobile Device

Software:
☐ Adobe Acrobat (full version) ☐ Email Encryption
☐ Microsoft Office Professional 2003 ☐ Microsoft Office Professional 2007
☐ MS Project 2007 ☐ MS Visio 2007 ☐ MS OneNote 2007
☐ Fax Server - *Specify level of access:*

☐ Miscellaneous Needs *(Enter any other requests)*:

TELEPHONY

Telephone:
☐ Desk Phone ☐ Softphone (IP Communicator)
☐ Desk phone currently exist at location. Current extension is:

Accessories:
☐ Wireless headset ☐ Wired headset

CELL PHONE / AIR CARD

☐ Cell phone ☐ Air Card

Accessories:
☐ Cell Phone Case/Holder ☐ Car Charger
☐ Miscellaneous Needs *(Enter any other requests)*:

BUILDING ACCESS

Access Requested for the following location(s):
☐ Medical Records Room ☐ Server Room
☐ Lobby ☐ Other, *Specify:*

Additional Access Restriction:
☐ After-Hours Access, *Specify Hours:*

Other Restrictions (be specific):

SPECIAL INSTRUCTIONS

Manager Checklist/Reminder:

- Signature below can be of the Department Head or the Data Owner if new network access is requested.
- Ensure employee badge is requested
- Schedule new employee orientation, if applicable
- Ensure name appears on any appropriate sign-in/out sheets
- Remember to have all new employees/contractors read and sign appropriate forms, i.e. Confidentiality Form (Appendix B)
- Request appropriate training/background:
    - HR Background Investigation
    - Security Training
    - Any additional training and/or background check

NAME	SIGNATURE	DATE
Department Head (Print Name)		
Security Officer/ Appropriate Authority		

15 Appendix B – Confidentiality Form

RESPONSIBILITY OF CONFIDENTIALITY

I understand and agree to maintain and safeguard the confidentiality of privileged information of Muslim Co-Operative Bank. Further, I understand that any unauthorized use or disclosure of information residing on the Muslim Co-Operative Bank information resource system may result in disciplinary action consistent with the policies and procedures of federal, state, and local agencies.

_____ _____

Date Signature

_____

Bank/Firm

_____ _____

Date Signature of Muslim Co-Operative Bank Privacy Officer

16 Appendix C – Approved Software

The following list has been approved for use by the Muslim Co-Operative Bank. All software must be installed and maintained by the appropriate Muslim Co-Operative Bank personnel.

Software	Version	Approved by	Date	Description/Comments

17 Appendix D – Approved Vendors

Vendor	Primary Contact	Main Number	Product / Service	Description/Comments

18 Appendix E – Breach Assessment Tool

PRIVACY BREACH ASSESSMENT

1) Was Private Information Involved? ☐ Yes ☐ No

2) Was the Private Information encrypted? ☐ Yes ☐ No

3) Description of breach:

a) What data elements have been breached?

b) What possible use is there for the private information? For instance, can the information be used for fraudulent or otherwise harmful purposes?

c) What was the date that the breach was discovered? _____

d) What is believed to be the date that the breach occurred? _____

2) Cause and Extent of the Breach

a) What is the cause of the breach?

b) Is there a risk of ongoing or further exposure of the information? ☐ Yes ☐ No

c) What was the extent of the unauthorized collection, use or disclosure, including the number of likely recipients and the risk of further access, use or disclosure, including in mass media or online?

d) Is the information encrypted or otherwise not readily accessible? ☐ Yes ☐ No

e) What steps have already been taken to minimize the harm?

3) Individuals Affected by the Breach

a) How many individuals are affected by the breach?

1. Who was affected by the breach:

☐ Employees

☐ Customer-owners

☐ Volunteers

☐ Contractors

☐ Service providers

☐ Other individuals/organizations

4) Foreseeable Harm from the Breach

a) Is there any relationship between the unauthorized recipients and the data subject?
☐ Yes ☐ No

b) Is any of the information or the individual whose information was compromised subject to additional protections, such as court orders, temporary restraining orders, protections from harm, etc.?

2. What harm to the individuals will result from the breach? Harm that may occur includes:

☐ Security risk (e.g., physical safety)

☐ Identity theft or fraud

☐ Loss of business or employment opportunities

☐ Hurt, humiliation, damage to reputation or relationships

☐ Other (please specify):

d) What harm could result to the organization as a result of the breach?

☐ Loss of trust in the organization

☐ Loss of assets

☐ Financial exposure

☐ Other (please specify):

e) What harm could result to the public as a result of the breach?

☐ Risk to public health

☐ Risk to public safety

☐ Other (please specify):