



# **IT Operations and Security Policy**

**(Version-III)**

**Directorate of Information Technology**

**Pakistan Bait-ul-Mal**

**Updated: April 2021**

## Table of Contents

1. Overview .....	3
2. Introduction .....	4
3. Acceptable Use Policy .....	5
4. Accessibility Policy .....	9
5. Hardware Security Policy.....	10
6. Auditing Policy.....	11
7. Backup Policy.....	13
8. Data Sharing Policy .....	16
9. Data Retention Policy .....	17
10. Electronic Communications Policy.....	18
11. Equipment Configuration Policy .....	19
12. Guest/Visitor Access and Technology Use Policy .....	20
13. Illegal File Sharing .....	21
14. Information Sensitivity Policy .....	22
15. Password Policy .....	25
16. Physical Security Policy.....	28
17. Personal Technology Service Policy .....	29
18. Remote Access Policy .....	31
19. Employee Rights and Responsibilities Policy .....	32
20. Surveillance Policy .....	33
21. IT Service Agreements Policy.....	34
22. Wireless Communication Policy .....	35
23. Internet accessibility Policy/Usage .....	36
24. Quality Control Policy for Data Entry.....	38
25. Operating Procedure - Directorate of IT .....	39
26. Equipment Procurement Procedure.....	40
27. Incident Management Procedure.....	41
28. Software Security and Managing Information System Policy .....	42
29. Disclaimer .....	47
30. User Create Form .....	48
31. Equipment Transfer Form.....	49
32. Incident Report Form .....	50
33. DATA ACQUISITION FORM.....	51
34. Handing Over /Taking Over .....	52
35. Policies and Procedures Manual Compliance .....	53
36. Non-Disclosure Agreement Form / Confidentiality Statement (For IT Personnel) .....	54
37. Authorization/Confidentiality Statement (For personnel using IFA e-filing BMS) .....	55

## 1. Overview

This document serves as a rulebook and roadmap for successfully and properly utilizing the technology resources at Pakistan Bait-ul-Mal (PBM). Careful consideration should be taken to verify that one's actions fall within the authorized parameters for access, utilization, distribution, and modification of technology resources set forth within this document.

The purpose of this policy is to establish Standard Operating Procedures (SOP's) for IT operations and ensure a minimum level of Security maintained by all Officers and officials that has access to computer hardware and IT-systems.

This manual provides the policies and procedures for selection and use of IT within the organization which must be followed by all employees. IT Directorate will use guidelines to administer these policies, with the correct procedure to follow and will keep all IT policies current and relevant. Therefore, from time to time it will be necessary to modify and amend some sections of the policies and procedures, or to add new procedures or update accordingly.

Any misuse, misappropriation, negligence, or deliberate disobedience concerning these policies and procedures will not be tolerated. It is up to each individual employee and affiliate of PBM to familiarize him/herself with the policies and procedures set forth or ask for guidance from IT Directorate.

## 2. Introduction

Most of PBM projects, financial, administrative, and Management data is accessible through the network. As such, they are vulnerable to security breaches that may compromise confidential information and expose the organization to losses and other risks. At all PBM locations, security is critical to the physical & logical network, database, computer operating systems, and application programs and each area offers its own set of security issues and risks.

This policy provides guidelines for the purchase of IT hardware for the organization to ensure that all hardware and technology for the organization is appropriate, value for money and where applicable integrates with other technology for the organization. The objective of this policy is to ensure that there is minimum diversity of hardware within the institution.

The privacy, accessibility, accountability, authentication, availability, reliability and Management Information system and network maintenance are components of a comprehensive security plan. In order to obtain secure environments for the working of a Computer based information system among other considerations, physical security measures to control and monitor the access to computer facilities play a very vital role. To exercise control on physical access to computer machine room and to regulate access to functional devices some physical security measures are vitally important. Software security is another key factor which contributes a lot in maintaining secured environments for any data processing activity. All the officers concerned must recommend suitable security classification and instructions for their programs.

### 3. Acceptable Use Policy

#### Overview

This policy establishes the acceptable usage guidelines for all PBM-owned technology resources. These resources can include, but are not limited to, the following equipment:

- i. Computers
  - Desktop Computers, Laptops, Mobile Devices, Servers, etc.
- ii. Network Equipment
  - Switches, Routers, Network and Communications Cabling, Wall Plates, Wireless Antennas, Wireless Bridge Devices, Fiber Optic Lines, Fiber Optic Equipment, etc.
- iii. Printing equipment
  - Printers, Scanners etc.
- iv. Audio/Video Equipment
  - Video Codecs, HDTVs, Document Cameras, Projectors, Security Cameras, Miscellaneous Cabling, Digital Cameras and Camcorders, etc.
- v. Software
  - Operating Systems, Application Software, etc.
- vi. Resources
  - Group Drive File Storage, Website File Storage, Email Accounts, Social Networking Accounts, etc.

This policy applies to all employees, consultants, and other workers at PBM. This policy applies to all equipment that is owned by PBM.

#### Policy

While PBM's IT Department desires to provide a reasonable level of freedom and privacy, users should be aware that all PBM-owned equipment, network infrastructure, and software applications are the property of PBM and therefore are to be used for official use only. Also, all data residing on PBM-owned equipment is also the property PBM and therefore, should be treated as such, and protected from unauthorized access.

The following activities provide a general roadmap to use PBM's technology resources in an acceptable manner:

- i. All passwords used to access PBM systems must be kept secure and protected from unauthorized use.
- ii. No user account can be shared between individuals. Authorized users are responsible for the security of their own passwords and accounts.
- iii. Do not transfer personally identifiable information on portable equipment and storage devices.

- iv. Public postings by employees from a PBM email address should contain the following disclaimer stating that the opinions expressed are strictly their own and not necessarily those of PBM, unless the posting is in the course of business duties:
  - Any views or opinions presented in this message are solely those of the author and do not necessarily represent those of PBM. Employees of PBM are expressly required not to make defamatory statements and not to infringe or authorize any infringement of copyright or any other legal right by electronic communications. Any such communication is contrary to PBM policy and outside the scope of the employment of the individual concerned. PBM will not accept any liability in respect of such communication, and the employee responsible will be personally liable for any damages or other liability arising.
- v. All computers residing on the internal PBM network, whether owned by the employee or PBM, shall be continually executing approved virus-scanning software with a current, up-to-date virus database.
- vi. Employees must use extreme caution when opening e-mail attachments received from unknown senders.
- vii. Personally identifiable information cannot be sent via electronic means and should be transferred within the internal network or through secure VPN connections.
- viii. Off-campus work should be completed via a secure VPN connection or secure login over the internet so that no data is transferred off-network.
- ix. All workstations should be kept secure. Users should lock the workstation when not attended to protect unauthorized users from accessing secure files.

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of PBM authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing PBM-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

The following activities are strictly prohibited, with no exceptions:

- i. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by PBM.
- ii. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which PBM or the end user does not have an active license is strictly prohibited.

- iii. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- iv. Introduction of malicious programs into the network or server environments (e.g., viruses, worms, Trojan horses, rootkits, etc.).
- v. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- vi. Using a PBM computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- vii. Making fraudulent offers of products, items, or services originating from any PBM account.
- viii. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- ix. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- x. Port scanning or security scanning is expressly prohibited unless prior notification to the PBM IT Directorate is made.
- xi. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- xii. Circumventing user authentication or security of any host, network or account.
- xiii. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- xiv. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- xv. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- xvi. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- xvii. Unauthorized use, or forging, of email header information.
- xviii. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- xix. Use of unsolicited email originating from within PBM's networks or other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by PBM or connected via PBM's network.

In order to ensure the authorized usage of Computer equipment, the following procedure may be observed:-

- i. **PCs and Printer:** The custodian of the Computer machine may be made personally responsible for any physical damage to it and may only use it according to the explained procedures for their individual systems.
- ii. The end user may also make sure that no un-authorized person is allowed to operate the machine and it is not left un-attended when it is practically functional. For a temporary pause, the user may make sure that he/she has switched-off the machine before leaving the room.
- iii. Any effort to access the other areas of Computer equipment by "hit and trial" method by anyone may be viewed as very serious violation and strict disciplinary action may be taken in this regard.
- iv. To maintain the privacy of Computer equipment, the password will be the personal responsibility of the user and in case of any doubt about its exposure, the password should immediately be changed.
- v. For sensitive data, strict security measures may be adopted according to its classification for Computer stored data and the source document.
- vi. **Laptop:** Following officials of PBM are authorized to use Laptop in the execution of their duty:-
  - Managing Director, DMD & Directors are entitled to use latest laptop. Any other staff member whose peculiar job necessitates the usage of laptop is authorized to keep laptop with the approval of Director (IT).
  - During the high-level presentation at conference room or outside [if required] by the executives of PBM with the approval of Director (IT).
- vii. Each District Office, WEC, SRCL, DuEs, Panahgahs, Meal on Wheels or any new project of PBM is entitled to keep one computer system/laptop alongwith scanner, printer, UPS, Attendance machine etc. Before deployment at above said locations, each PO/RO will ensure the IT Training of nominated resources with the consultation of IT Directorate, Head Office.



## 4. Accessibility Policy

### Overview

This policy establishes the accessibility guidelines for all PBM-owned technology resources. The purpose of this policy is to ensure that everyone is presented with an equal opportunity to learn and that all employees can adequately use the required technology equipment for the purpose of their required occupation.

### Policy

The PBM IT Department will always strive to offer technology solutions that help improve the learning environments for all employees but will be particularly diligent in ensuring that no employee will be unable to learn.

The PBM IT Department cannot be held liable for issues surrounding software application issues, hardware failures, or the inability to use IT resources.

With that said, the PBM IT Department will continually strive to ensure that all offices have the necessary technology and are adequately structured in a way to provide the most conducive environment.

## 5. Hardware Security Policy

Opening /Closing Measures Opening and closing timings are more critical from over-all security point of view and special treatment must be provided to these procedures for safeguarding against any potential risk involved. These may include:-

- i. Keys of the Room where Computer is installed such as **server room, computer Lab**, may be personally collected/deposited by the official authorized for the same, daily from the duty room as per laid down procedure.
- ii. The temperature, cleanliness and dust proof arrangements with regard to Computer equipment may be maintained accordingly.
- iii. Computer may be switched-on/off according to the specified procedure by the authorized officials specially deputed for this job only.
- iv. In case mal-functioning of any device is observed, matter may be immediately reported to the concerned officer for taking necessary remedial measures.
- v. Before switching off the Computer the in-charge must ensure that: -
  - No computer output is left unattended,
  - All diskettes /CD and other storage media have been placed under secured environment.

Access to Computer Machine The main responsibility of controlling access to the Computer machine may, be of In charge of the room, where Computer is installed, and he may discharge this duty with the assistance of officials under him. As a result of this control, the following may be exercised strictly:-

- i. No un-authorized person may be allowed to handle the Computer equipment.
- ii. Even the staff members working in that set-up, but not associated with the Computer Operation, may not be allowed to operate the Computer equipment.

All Computers and Printers have been distributed to each branch on temporary basis. No equipment will be shifted / replaced to other branch without the approval of Director (IT). No equipment will be changed / replace even with in branch without the consent of IT Directorate. Unauthorized shifting of any computer hardware from one place to the other is strictly prohibited and liable to disciplinary action against defaulters, as deemed fit by the competent authority. In case of theft OR any other misappropriation relating to computer hardware/software, immediately inform Directorate of IT for further necessary action.

## 6. Auditing Policy

### Overview

This policy addresses third-party entities and their ability to conduct an internal technology audit. This type of audit is basically a “stress-test” on our technology resources to evaluate the level of security our technology systems present as well as the level of scrutiny it can withstand.

Vulnerabilities are a primary focus for the PBM IT Department. Seeking these vulnerabilities out before they develop into potential problems is best for PBM, its resources, employees and associates. To accomplish this, internal audits are necessary to periodically determine what vulnerabilities may exist within PBM’s technology resources.

The purpose of this agreement is to set forth a policy regarding network security scanning offered by a third-party audit group to PBM. The PBM IT Department shall allow the utilization of various methods (both hardware and software) to perform electronic scans of our networks, firewalls, hardware devices and MIS located/hosted at PBM or external Server.

Audits may be conducted to:

- i. Ensure integrity, confidentiality and availability of information and resources
- ii. Investigate possible security incidents to ensure conformance to the established PBM IT Department’s security policies
- iii. Monitor user or system activity where appropriate

### Policy

This policy covers all computers, equipment, and communication devices owned or operated by PBM. This policy also covers any computers, equipment, and communications devices that are present on PBM premises, but which may not be owned or operated by PBM. The third-party audit group will not perform Denial of Service activities at any time during an audit.

When requested, and for the purpose of performing an audit, consent for the access required to perform the scan will be provided to members of the third-party audit group by the PBM IT Department. The PBM IT Department hereby provides its consent to allow the third-party audit group to access its networks, firewalls, hardware devices and MIS to the extent necessary to perform the scans authorized in this agreement. The PBM IT Department shall provide protocols, addressing information, access to MIS and network connections sufficient for the third-party audit group to perform network scanning and to run quality test on MIS.

The access involved in the scan or test may include:

- i. User level and/or system level access to any computing, networking equipment, and communications devices.
- ii. Access to information (electronic, hardcopy, etc.) that may be produced, transmitted, or stored on PBM equipment and/or premises.
- iii. Access to work areas (labs, offices, cubicles, storage areas, etc.)
- iv. Access to interactively monitor and log traffic on PBM networks.
- v. Access to MIS to run testing process.

Since PBM gains access to certain resources from third-party entities, cooperation from these resources may be required to perform a full network scan. For instance, NAYATEL or any other DSL/Broadband Service Provider provides the Internet connections to the PBM networks. Because of this, a comprehensive network scan may require the assistance of DSL/Broadband Service Provider or other third-party service providers should part of the scanning activities originate outside the PBM network.

Network performance and/or availability may be affected by the network scanning. The PBM IT Department releases any third-party audit group of any and all liability for damages that may arise from network availability restrictions caused by the network scanning, unless such damages are the result of the third-party audit group's gross negligence or intentional misconduct.

MIS Quality Control shall be made in accordance with the standards and procedure and third-party audit group will use the testing software/applications to assure the quality of MIS and reliability of data stored into Servers.

The PBM IT Department shall identify, in writing, a person to be available should the third-party have questions regarding data discovered or should the third-party require assistance.

PBM and the third-party audit group shall identify, in writing, the allowable dates for the audit vulnerability scan or test to take place. Permission to conduct a vulnerability scan or test will be obtained from the Director of IT and the Managing Director (MD) a minimum of 48 hours prior to the test.

Internal IT Audit will be conducted by IT Directorate Head Office and visit will be planned accordingly to inspect or evaluate the optimal utilization of IT resources at PO/RO/DO or any other projects/schemes. Concerned PO/RO IT Branch may also conduct the IT audit of their respective Provincial/Regional Office/District Office/projects/Scheme with the approval of competent authority.

## 7. Backup Policy

### Overview

The PBM IT Department maintains systems to hold and retain all essential data for each individual department. This storage area, or group drive as it is referred to, is used to securely store all data for any given department. Because of this centralized storage arrangement, the PBM IT Department is able to offer secure backup capability ensuring all data will be accessible in the event of a disaster or other event in which the data would be destroyed.

This policy establishes regular backup schedules for our group drive storage devices and pertains to all this data. With that said, this does not pertain to individual, departmental, or computer lab devices, mobile devices, or other portable storage medium where the data resides locally on the device or medium. The PBM IT Department does not guarantee backup for any of these types of devices or storage medium.

### Policy

Every effort shall be made by the individual departments and employees at PBM to store sensitive, important, and confidential data on their respective group drive. As mentioned above, the PBM IT Department cannot be held liable for issues with data stored elsewhere.

Regular backup schedules are in place within the group drive storage device to ensure that backups occur at regular intervals and over a time span to provide ample opportunity for the PBM IT Department to recover a file, folder, or group of such. It should be noted that the PBM IT Department does require immediate notification in the event a file, folder, or collection of either is found to be missing, corrupt, or otherwise damaged. Waiting to inform the PBM IT Department decreases the probability of successful recovery.

Specific information regarding backup restoration on an institution scale can be found in the PBM IT Department's Disaster Recovery Plan (DRP) or the associated Backup Priority List (BPL). These deal with catastrophic recovery needs that affect multiple departments or the institution as a whole.

The hardware that the PBM IT Department uses consists of two storage devices. One device is placed in the server area of the IT Department to serve as a primary storage backup device while the other is placed in the server area of remote site to serve as an off-site backup and replication device. PBM IT Department will keep the backup in 02 types of media storage i.e. NAS (Network Attached Storage) and external hard-disks in Head Office.

The primary device holds all data and backups and serves as the primary device for file access and immediate backup. The secondary, off-site device replicates all data to create a stable off-site copy of the data.

For this document, considering the type of hardware described above, normal backups do not necessarily retain the same meaning as when used in conjunction with other hardware devices. Because of this, the following descriptions are provided, based on the current hardware being used, so as to better understand the overall backup process.

- i. **Backups:** These refer to snapshots taken of the file structure and database. These snapshots are essentially pointers to changes occurring within the storage device since the last scheduled snapshot. This greatly reduces the file storage requirements necessary to hold backups while still providing the same or superior level of backup capability found in other devices.
- ii. **Replication:** This refers to the copying process of all data and associated backups from the primary backup device to the secondary backup device. During a replication, all data and backups are replicated so that a mirror copy is retained for off-site, backup capability should a disaster or other issues occur.

Regularly scheduled backups and replications shall be performed by the concerned Assistant Director of PBM IT Department. IT Department will ensure to perform Weekly/Monthly/Mid-Yearly/Yearly backups and store at a secure location. All backups shall be clearly labeled so as to distinguish one from another easily.

Testing for data integrity will be performed at regularly scheduled intervals by the backup hardware but may also be performed manually at random times to verify the validity, accuracy, and authenticity of the backup. These random tests should total no less than six per year and it is recommended that these tests fall approximately two months apart, less if more than the minimum number of tests are used.

We encourage that backup tests be taken within one week of the completion of the yearly and mid-yearly backups with the remaining backups spaced throughout the remaining months of the year. If six are used, it should follow this testing schedule:

If more than six tests are used, then the schedule may be set at the discretion of the PBM IT Department, however, two of the tests must occur no later than one week after the yearly and mid-yearly backups are completed.

Testing shall consist of one or more of the following methods of data validation and verification of accuracy and authenticity:

- i. **Random Dummy File Restoration:** Six to twelve dummy files are inserted on the file server at random locations. Afterwards, we will intentionally delete these dummy files. Then, recovery will be tested to verify data is being restored properly. If this verifies the data is being restored properly, the test is completed and the dummy file may be removed.
- ii. **Random Actual File Restoration:** Recovery of a six to twelve actual random files located on the server. Comparisons will then be made with current versions of the same files to verify content and accuracy of restoration process. If the comparisons verify that the recovery was successful, then the test is completed.
- iii. **Random File Location Verification:** Movement of a single dummy file to various locations on the file server. Initially the file is inserted onto the file server and backups are tested to verify the file exists in backups at the initial location. If this is confirmed, then the file is moved on the file server to a second location and backups are tested yet again to verify that the file is in the second location. Once this is confirmed, the file is moved for a third time and backups are once again tested to verify the file exists in the new location. If this is confirmed then the test is completed and the dummy file may be removed. Backups are working correctly and file contents and locations are being updated appropriately.

- iv. **Miscellaneous:** Other tests may be used at the discretion of the PBM IT Department with only one restriction: they may not interfere with access or otherwise cause any data loss on the file server.

All restoration processes will follow, at minimum, one of the following methods:

- i. Re-routing primary traffic from backup and storage device to accompanying device or vice-versa
- ii. Physically transporting one device to another location
- iii. Copying all files or a subset of files from the backup equipment to the file server
- iv. Via the testing process described in this document
- v. Utilizing the PBM IT Department's Disaster Recovery Plan
- vi. Utilizing the PBM IT Department's Backup Priority List
- vii. Other methods, approved by the PBM IT Department, that do not interfere with access or otherwise cause any data loss on the file server

If it is found that a scheduled backup process is incomplete or missing due to a hardware or software malfunction, then the backup will be completed as soon as possible and a hardware test will be needed to verify no long-term problems exist that may affect backups in the future. Should a hardware test yield results that indicate serious issues, then a replacement for the faulty hardware should be found as soon as possible in order to prevent such issues from occurring in the future.

If these issues prevent backups from occurring, then the off-site backup device will be transferred to primary backup duties and a secondary device should be purchased (if not available) and then placed to regain primary functionality.

Online log files are retained consisting of information for each backup or replication process, hardware/software errors, access issues, or other critical errors involving the backup hardware. These entries are also emailed to the PBM Backup email account for verification and notification.

## 8. Data Sharing Policy

### Overview

IT Directorate is the custodian of databases and will only share with authorized stakeholders/users. This policy will determine data sharing guidelines and authenticity of data. Data will be shared on demand after approval by the competent authority.

### Policy

- i. All branches are required to send the request and parameters on “Data Acquisition form” with proper justification and prior approval of DMD/Director Admin/Branch Incharge;
- ii. Data sharing in MS Excel/MS Word format will be discouraged;
- iii. In case of data required to be shared outside PBM, only the PDF format will be used;
- iv. In case of report exceeding 20 pages, data will be provided in PDF format on CD;
- v. Minimum response time to provide required report will be one (01) working day;
- vi. Branches will be responsible for safe custody of shared data;
- vii. Required report will be provided by IT Directorate through approving authority;



## 9. Data Retention Policy

### Overview

This policy will determine how long data shall be retained under the guidelines of federal government law and within institutional policies.

### Policy

The data of current/on-going projects will be available, however data of closed schemes/projects will be archived for maximum 05 years. The data in common drives will be stored for temporary purpose, and will be deleted after some time.

Under no circumstances is data to be removed, discarded, disposed of, or otherwise destroyed that will compromise legal compliance, data integrity, or institutional needs. The PBM IT Department shall make every effort to extend the data retention timeframes of all data as long as the institution requires access without compromising any legal statutes set forth regarding storage or destruction of such data. No data will be destroyed prior to or retained longer than any legal requirement dictates.

The PBM IT Department will continually utilize backup equipment, secondary-site storage, and regular backup schedules to ensure that critical data is retained and kept from corruption or other types of data loss. Every effort shall be made to ensure the institutional data needs are given top priority in the event of a loss of data, corruption of data, or if data recovery is necessary.

This policy shall never decrease the retention time under any federal law but may only increase the retention timeframe required by the institution. This increase may only be applicable as long as it does not compromise the integrity, storage capability, or otherwise degrade the overall storage capability of the system being used.

## 10. Electronic Communications Policy

### Overview

Electronic communication is necessary to fulfill multiple roles and activities here at PBM. Because of the varying types of electronic communication, we will focus on those used primarily here at PBM:

- i. Email
- ii. VoIP/IP Telephony
- iii. Videoconferencing

Email is the official method of communication at PBM, both for students and employees. Business is conducted every day via email. Since email has both positive and negative connotations, it is imperative that we recognize that the positive aspects greatly outweigh the negative aspects. However, we must also realize that the negative aspects exist and ensure that this method of communication is used effectively, efficiently, and for its' intended purpose.

PBM's VoIP/IP Telephony system is used to transmit and receive audio/video within the institution to facilitate direct communication amongst employees and departments. It is also used to transmit and receive audio outside the institution to facilitate direct communication with beneficiaries, other institutions, and other third-party entities. Because of this capability, we must ensure that it is used for work purposes.

Videoconferencing equipment is used primarily for meeting requiring connectivity to other PBM remote locations. Videoconferencing equipment is also used to facilitate conferences and meetings with other institutions, or other third-party entities. Since this type of communication conveys not only audio, but video as well, it is particularly important for it to be used for its intended purposes.

### Policy

Regardless of the type of technology being used, electronic communication is meant to serve the needs of the organization by sharing information with employees, individuals or other agencies. Because of the unique capabilities of each system it is important to realize that each type of communication method contains unique issues that must be addressed on a case-by- case basis; however, general rules can be set forth to ensure that any communication method is used wisely and according to its intended purpose and this sort of communication method shall never be used for the creation or distribution of any misleading information or any other illegal purpose.

In general, PBM's electronic communication mechanisms are to be used to share information with employees, individuals, and other agencies.

It is also important to note that the true definition of information sharing at PBM is to adequately convey the appropriate knowledge so that the organization mission is not hindered but enhanced. This information is always to be distributed under the following assumptions:

## 11. Equipment Configuration Policy

### Overview

This policy has been established to create a standard configuration for all technology resources at PBM. Because of the variances between the types, makes, models, configurations, builds, versions, and brands of technology resources available, it is necessary to standardize all technology resources to make service and maintenance easier and also to help keep costs down.

### Policy

All employees shall order and utilize equipment that is serviceable and recommended by the PBM IT Department. Since equipment availability changes over time, especially when referring to technology, a comprehensive list indicating appropriate hardware would be virtually impossible to create. Because of this, any individual or department wishing to purchase technology equipment should first consult a PBM IT Department personnel member for current specifications for any given piece of equipment.

This applies to all technology equipment.

For more details on procedures required to place an order for technology equipment, please see the Equipment Procurement Procedures included in this document for detailed instructions.

## 12. Guest/Visitor Access and Technology Use Policy

### Overview

PBM maintains an atmosphere that is open and allows guests and visitors access to resources, as long as such access does not compromise the integrity of the systems or information contained within the premises and does not introduce malicious software or intent to the internal network.

### Policy

Guest and visitor access shall be classified into two types as described below:

- i. Standard – Access granted to internet resources and institutional resources located online.
- ii. Special – Access granted above plus any internal access as requested by an individual with the authority to do so:
  - Vice President for Fiscal Services, Vice President for Academic Affairs, President, or other designee deemed necessary by the President

Internal Access may include:

- i. Wireless VLANs (i.e. PBMwireless, PBMguest)
- ii. Wired VLANs (i.e. housing, guest)
- iii. Singular or multiple file access
- iv. System access such as Blackboard, ID Card System, etc.

Under no circumstances should visitors be given special access unless permission has been obtained from the appropriate administrative personnel (i.e. a signature from one of the personnel above) along with detailed description of access.

To obtain guest/visitor access users should contact the PBM IT Department with their requested system access requirements using the attached Authorization of User Access form.

## 13. Illegal File Sharing

### Overview

Legal compliance is a primary focus at PBM. Because of this, we have set forth this policy which addresses illegal file sharing legislation, legal alternatives to illegal file sharing, and penalties for violating state and federal copyright laws.

This policy applies to all PBM employees, students, vendors, or visitors utilizing PBM-owned computers, equipment, or the PBM network.

### Policy

File sharing (peer-to-peer) software programs have led to significant increases in anti-piracy efforts and legislation. Peer-to-peer software allows the sharing of files often consisting of copyrighted content such as music, movies, and software which usually occurs without the consent of the owner.

It is the policy of PBM to respect copyright ownership and protections given to authors, owners, publishers, and creators of copyrighted work. It is against PBM policy for any employee, affiliate, or visitor to copy, reproduce, or distribute any copyrighted materials on PBM-owned equipment or the PBM-managed network unless expressly permitted by the owner of such work.

PBM also discourages the use of any file-sharing program as these types of programs may allow copyrighted material to be downloaded to a PBM-owned computer or device. Many of these programs automatically place downloaded files in a shared folder on your computer, which means you could be sharing files without your knowledge. This also means that you may be held responsible for illegal file sharing, whether you are aware that copyrighted files are being shared or not.

PBM also employs the use of network appliances, equipment, and rules to limit the amount of file-sharing traffic on the PBM network. Active blocking of peer-to-peer traffic is used to protect the PBM network from unwanted traffic and the presence of potentially malicious files introduced through file-sharing programs.

PBM encourages employees, affiliates, and visitors to utilize legal alternatives to illegal file sharing. There are a variety of free and pay-per-use options available that can be used instead of illegal file sharing programs. Several of these free and pay-per-use options are listed below; however, this is in no way an all-inclusive list. PBM leaves it to the discretion of the employee, affiliate, or visitor to decide which alternative to utilize. They are provided herein for reference only and PBM does not endorse or provide any guarantee or support for any of the legal alternatives located below.

## 14. Information Sensitivity Policy

### Overview

Information sensitivity is a primary focus at PBM. Since we are a government entity, we deal with many different types of information, some for public use, some not. To make these distinctions, this document will address both types of information.

This policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of PBM without proper authorization.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as via phone and videoconferencing).

All employees should familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect confidential information (e.g. confidential information should not be left unattended in conference rooms.).

NOTE: The impact of these guidelines on daily activity should be minimal.

Questions about the proper classification of a specific piece of information should be addressed to your supervisor or the PBM IT Department. Questions about these guidelines should be addressed to the PBM IT Department.

### Policy

By grouping information into two different categories, we can adequately address the needs of each type of information. The first type, public Information, is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to the institution. The second type, confidential information contains all other information. It is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Included is information that should be protected very closely, such as specific personnel information, employee data, projects/schemes data, etc. Also included in confidential information is information that is less critical, such as telephone directories, personnel information, etc., which does not require as stringent a degree of protection.

A subset of the latter is third-party confidential information. This is confidential information belonging or pertaining to another corporation which has been entrusted to PBM by that company under non-disclosure agreements and other contracts. Examples of this type of information include everything from joint development efforts to vendor lists, customer orders, and supplier information. Information in this category ranges from extremely sensitive to information about the fact that we've connected a supplier / vendor into PBM's network to support our operations.

PBM personnel are encouraged to use common sense judgment in securing confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their supervisor and/or the PBM IT Department for more information and instructions on how this information should be handled.

The sensitivity guidelines below provide details on how to protect information at various sensitivity levels. Use these guidelines as a reference only, as PBM Confidential Information at each level may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the PBM Confidential Information in question.

i. Minimal Sensitivity

- Description: General information, some personnel, and technical information.
- Access: PBM employees, associates, or third-parties with a business need to know.
- Distribution internal to PBM: Approved electronic mail and approved electronic file transmission methods.
- Distribution external to PBM: Approved electronic mail and approved electronic file transmission methods.
- Storage: When viewing data, do not allow viewing by unauthorized individuals. Do not leave data open and/or unattended in any format. Protect data from loss, theft, or misplacement. Electronic information should have individual access controls where possible and appropriate.
- Disposal/Destruction: Electronic data should be permanently expunged or cleared.
- Reliably erase or physically destroy media. Data retention policy and federal and state retention guidelines should be observed for original copies.

ii. More Sensitive

- Description: Business, financial, technical, and most personnel information.
- Access: PBM employees, associates, or third-parties with signed non-disclosure agreements with a business need to know.
- Distribution internal to PBM: Approved electronic file transmission methods.
- Distribution external to PBM: Approved electronic file transmission methods via a private link to approved recipients external to PBM locations.
- Storage: Individual access controls are highly recommended for more sensitive electronic information.

- Disposal/Destruction: Electronic data should be permanently expunged or cleared.
- Reliably erase or physically destroy media. Data retention policy and federal and state retention guidelines should be observed for original copies.

iii. Most Sensitive

- Description: Operational, personnel, financial, source code, & technical information integral to the security of the institution.
- Access: Only those individuals (PBM employees and associates) designated with approved access and signed non-disclosure agreements.
- Distribution internal to PBM: Approved electronic file transmission methods.
- Distribution external to PBM: Approved electronic file transmission methods to recipients within PBM. Strong encryption is highly recommended.
- Storage: Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored on a physically secured computer.
- Disposal/Destruction: A necessity. Electronic data should be permanently expunged or cleared. Reliably erase or physically destroy media. Data retention policy and federal and state retention guidelines should be observed for original copies.



## 15.Password Policy

### Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of PBM's entire network. As such, all PBM employees (including contractors and vendors with access to PBM systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

The policy is applicable to all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that belongs to PBM, resides at any PBM location, has access to the PBM network, or stores any PBM information.

### Policy

All passwords will meet the following criteria:

- i. All system-level passwords (e.g., root, admin, application administration accounts) must be changed at least every 180 days.
- ii. All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 120 days.
- iii. User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- iv. Passwords must NOT be inserted into email messages or other forms of electronic communication.
  - Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
  - All user-level and system-level passwords must conform to the guidelines described below.

Passwords are used for various purposes at PBM. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Very few systems have proper support for one-time tokens (i.e., dynamic passwords that are only used once); therefore, every PBM employee should know how to select strong passwords.

Poor, weak passwords have the following characteristics:

- i. The password contains less than eight characters
- ii. The password or a subset of the password is a word found in a dictionary (English or foreign)
- iii. The password is a common usage word such as:
  - Names of family, pets, friends, co-workers, fantasy characters, etc.

- Computer terms and names, commands, sites, companies, hardware, software
- The words "PBM" or any derivation
- Birthdays and other personal information such as addresses and phone numbers
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards
- Any of the above preceded or followed by a digit (e.g., secret1,

1secret) Strong passwords have the following characteristics:

- i. Contain between 8 and 32 characters
- ii. Contain both upper and lower case characters (e.g., a-z, A-Z)
- iii. Contain at least one number (e.g., 0-9)
- iv. Contain special characters (e.g., ~, !, @, #, \$, ^, (, ), \_ , +, =, -, ?, or ,)
- v. Does not contain a dictionary word in any language, slang, dialect, jargon, etc.
- vi. Does not contain personal information, names of family, etc.

Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Please do not use either of these examples as passwords!

Do not use the same password for PBM accounts as for other non-PBM access (e.g., personal ISP account, option trading, benefits, etc.). Do not share PBM passwords with anyone. All passwords are to be treated as sensitive, confidential PBM information.

Here is a list of "don't's":

- i. Don't reveal a password over the phone to ANYONE.
- ii. Don't reveal a password in an email message.
- iii. Don't reveal a password to a supervisor.
- iv. Don't talk about a password in front of others.
- v. Don't hint at the format of a password (e.g., "my family name").
- vi. Don't reveal a password on questionnaires or security forms.
- vii. Don't share a password with family members.
- viii. Don't reveal a password to co-workers.
- ix. Don't reveal a password to vendors.
- x. In short, don't reveal a password to ANYONE.
- xi. Do not use the "Remember Password" feature of applications (e.g., Eudora, OutLook, Netscape Messenger, Internet Explorer, Firefox, Thunderbird).
- xii. Do not write passwords down and store them anywhere in your office.

- xiii. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without proper encryption.
- xiv. Change passwords at least once every three months.

Other items to remember:

- If someone demands a password, refer them to this document or have them call the PBM IT Department to determine the validity of their request.
- If an account or password is suspected to have been compromised, report the incident to the PBM IT Department immediately and change all passwords as soon as possible.

Password cracking or guessing may be performed on a periodic or random basis by the PBM IT Department or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

Never give your password out to anyone. This may or may not include your supervisor, a friend or relative or part-time worker, or even a co-worker.

## 16. Physical Security Policy

### Overview

This policy will establish physical security guidelines that apply to all computing and networking equipment locations. It is important to note that incremental degrees of security will be needed for each area depending on the actual equipment configuration and critical need to the institution.

### Policy

All areas will be classified into two categories:

- i. Office
- ii. Restricted

Office areas are simply that, office locations for PBM IT Department employees. These areas contain computing equipment and other data that should be protected at all times.

Restricted areas are those areas that belong to the PBM IT Department and contain equipment owned and/or operated by the PBM IT Department or a third-party vendor (i.e. OneNet) such as:

- i. Server rooms
- ii. Switch closets
- iii. IT Department storage areas

At the time of this policy, our current physical security offerings are somewhat limited so more advanced options cannot currently be used. As upgrades occur, recommended options will be changed to required options to increase and enhance security.

All PBM IT Department restricted and office locations should contain the following recommended security mechanisms:

- i. Keyed locks
- ii. Face recognition-based access or ID card access

## 17. Personal Technology Service Policy

### Overview

This policy will set forth the rules and regulations which will determine how the PBM IT Department personnel are to perform work on personally-owned employee technology products.

The PBM IT Department does not service technology equipment for individuals who are not PBM employees.

### Policy

The PBM IT Department always strives to ensure that PBM employees, students, affiliates, and visitors receive the best possible technology assistance available for us to provide. However, this can leave something to be desired for non-PBM, personally-owned technology equipment owned by employees, students, affiliates, and visitors.

This policy will set forth the rules, regulations, and guidelines for which the PBM IT Department personnel may provide services for personally-owned technology equipment and/or projects outside of normal work hours.

NOTE: All technology requests for configuration or connectivity to the PBM network from personal technology devices will be handled at no cost. This policy applies only to technology issues related to the personal needs of the user.

All requests for personal technology assistance will begin with a preliminary diagnosis and troubleshooting process which is provided for FREE. If additional work is authorized by the user then the accompanying Personal Technology Service Policy Consent Form must be read and signed before any work may begin.

The PBM IT Department offers no implied warranty or guarantee on any work performed on personal technology equipment. All work is performed as-is as a service to our employee and as a cost-saving alternative for their benefit. However, it is beneficial to note that all work is performed on the same level as comparable service on PBM owned equipment.

All personal technology work will be performed within the following restrictions:

- i. Personal technology work may be performed during regular business hours, only if such work does not directly interfere or delay the normal operations or job duties of the PBM IT Department employee.
- ii. No on-site work. All equipment must be brought to the PBM IT Department for a preliminary diagnosis and troubleshooting.
- iii. No parts purchases. All parts to be installed must be purchased by the user.

- iv. No illegal software. Only legally licensed software may be installed.
- v. No work without proper authorization signature on consent form.

All issues should be expected to take approximately 24-48 hours to complete; however, they may take longer depending upon the severity of the problem at hand. Please expect to leave any equipment for a minimum of 48 hours for proper problem resolution.

PBM cannot be held responsible for any work done after hours by PBM IT Department personnel on any personal technology equipment. All work provided is not warranted or guaranteed. By signing the Personal Technology Service Policy Consent Form, you agree to these terms and conditions and waive any damages which may occur due to any work on your personal technology equipment. All work is done and once completed is left as is and no standing warranty or guarantee is implied.

## 18.Remote Access Policy

### Overview

This policy establishes the official rules set forth to allow users to remotely access and manipulate personally identifiable information, network applications, and other data from off-campus.

### Policy

Any user who seeks to work off-campus for the purpose of working from home or at another location can facilitate this through the use of the PBM or VPN connection. All users needing access to applications requiring network connectivity to the office can facilitate this by connecting from home via a VPN connection.

This type of connection establishes a secure, encrypted connection, to the campus network to allow the user to manipulate and access the data at a distance. If a given user wishes to work while off-campus, he/she should use the enclosed Remote Access Procedure to obtain a secure connection to the network and work from a distance.

This type of connection allows the user to remotely manipulate and access the data without actually transferring any data off-site thus ensuring all data is kept safe and secure from unauthorized access.

## 19. Employee Rights and Responsibilities Policy

### Overview

It is the understanding of all students, upon being admitted to PBM, that the technology resources and equipment provided are for the benefit of all employees. This policy explains what rights students have with respect to this technology and also what responsibilities are expected of each student.

### Policy

Every student that attends PBM shall be given an equal opportunity to learn and equal access to technology to help facilitate learning. All employee, regardless of major, classification, employee-type, housing location, or other identifying factor shall receive the same technology access as any other employee.

Employees should expect to receive access to wireless connections in offices, common areas etc. Employees should also expect up-to-date computers in labs and teaching areas, multimedia equipment in most classrooms, state-of-the-art instructional television classrooms, and easily accessible online systems such as Online applications, PBM e-mail etc. Employees should also expect to receive reliable, free internet service while on campus at speeds unobtainable through any normal Broadband/ISP.

With all of these rights and amenities, the PBM IT Department does make some responsibilities and assumptions of our employees. These responsibilities are as follows:

- i. Employees are expected to utilize their PBM e-mail address as it is the official method of communication with PBM.
- ii. Employees are required to safeguard login credentials and not share user accounts.
- iii. Employees are expected to respect others privacy and equipment.
- iv. Employees are expected to use only permissible equipment on campus:
  - a. Computers such as laptops, desktops, mobile devices, etc.)
- v. Employees are to observe prohibited devices in dorm areas:
  - a. Personal routers, wireless access points, bridges, or other network equipment.
- vi. Employees are expected to observe all local, state, and federal laws concerning technology.
- vii. Employees are required to comply with all policies included in this document.



## 20. Surveillance Policy

The purpose of the Workplace Surveillance Policy is to ensure that a transparent environment exists within the premises with regard to surveillance.

Each Provincial/Regional Office (PO/RO) or Projects/Scheme Office will provide the approval for the installation and deployment of CCTV cameras to the IT Directorate or IT team in PO/RO. IT Directorate at HO or IT Team at PO/RO will ensure the deployment of security cameras in the office premises and responsible for relevant technical support.

Security Office, PBM with coordination of Admin Branch and IT Department will ensure proper installation of high-resolution night vision security cameras with minimum 07 days recording storage capacity. Proper monitoring mechanism shall be devised by Security Officer, PBM.

## 21. IT Service Agreements Policy

This policy provides guidelines for all IT service agreement entered into on behalf of the PBM. IT Service Agreement will be required for hiring the IT services from IT Contractors/firm/vendor.

- Provision of network hardware and software
  - Development and Deployment of Software
  - Repairs and maintenance of IT equipment
  - Provision of all types of IT equipment.
  - Maintenance of IT Equipment.
  - Hiring of IT services
  - Any other IT related Software/Hardware
- 
- i. IT service agreements must be approved by the competent authority after reviewed and vetted by the Legal department.
  - ii. Renewal of IT service agreements will also be required.
  - iii. In the event that there is dispute to the provision of IT Services covered by an IT Service agreement, it must be referred to the Legal for settlement of such dispute.

## 22. Wireless Communication Policy

### Overview

Wireless implementations are a benefit to PBM employees. Maintaining this equipment can be a tedious process but is a necessity.

At present, this policy allows access to the PBM wireless network via any data communication device containing the hardware required to connect. Connecting to the PBM wireless network does not grant a user access to the internal networking infrastructure or any internal information of PBM, only external access to the internet. Utilizing PBM's wireless network for access to the internal network and/or information requires additional software that must be obtained through the PBM IT Department.

This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of PBM's wireless networking access points. This includes any form of wireless data communication device capable of transmitting packet data.

### Policy

All wireless data communication devices connected with PBM's wireless network will be required to have current virus-scanning software installed with the most recent updates and perform a full system scan a minimum of once per week.

All wireless data communication devices connected with PBM's wireless network that require access to PBM's internal network and/or information will be required to utilize specific software and/or access credentials obtained through the PBM ITS Department to do so.

At no time shall any device connected to the PBM wireless network operate outside the parameters defined in the Acceptable Use Policy provided herein. All wirelessly connected devices may be monitored and their information such as IP address, MAC address, general hardware profile, etc. be archived for future use. Random scans may also be performed to ensure the security of the wireless networks and connected devices and to obtain a general device survey to further enhance the accessibility and usability of PBM's wireless networks.

## 23. Internet accessibility Policy/Usage

### Overview

The PBM recognizes the value of the Internet as a powerful tool for research and communication, and would like to make this resource available for its employees and executives. In order to prevent misuse of this facility, the PBM sets down the following guidelines for its use.

**Rights: Access to the Internet is a privilege and not a right. This privilege may be withdrawn if anyone fails to show responsible behavior while using the Internet.**

- i. Keeping in view the security of Data and Applications hosted in the premises of PBM, the network security equipment i.e. Firewall must be installed.
- ii. All incoming ports from the outside world should be blocked by default. Only ports that are used by the applications to be opened for the outside world for proper functioning of Applications.
- iii. As per directions of Ministry of IT government of Pakistan social media applications i.e. Facebook, Whatsapp etc are prohibited for sharing of official data and confidential information.
- iv. Employees are encouraged to use the Internet for research in ways that promote the organizational goals of the PBM.
- v. Every computer user will be able to access the Internet provided that, if he/she is Assistant Director or above or otherwise authorised by concerned Director for specific job/research – for specific period only.
- vi. Internet users may copy research material (text, images etc but not downloaded executable files) from the Internet and save it in their private folders.
- vii. Internet users may access web-based personal e-mail accounts with permission from the immediate officer.
- viii. The Directorate of IT reserves the right to routinely monitor employee's folders to check the unnecessary material downloaded by the user.

**Responsibilities:** Internet Users should display responsible behavior for the use of computer equipment and other I.T. resources.

- i. You are not allowed to visit sites containing objectionable material (sexually explicit sites, hate sites, or those exhibiting violence or lewd language etc) or with any content that might be deemed damaging or unsuitable.
- ii. You should not try to hack into areas where access has been restricted – for example, others' private folders, sites or information which may be protected or confidential, or sites which have been banned in the PBM's filtering policy.
- iii. You may not send or receive e-mail which contains abusive, insulting, or sexually explicit language, or open attachments of any kind.
- iv. You should not use the Internet for chatting (unless granted special permission for organizational purposes) or for any other purpose which is deemed a waste of resources.

- v. You are not allowed to download any files from the Internet unless granted permission by the supervisor or immediate officer to do so.
- vi. You should respect international copyright laws when copying material from the Internet.
- vii. You should not use the Internet for political or commercial purposes.
- viii. You are not allowed to log into anyone else's account. If someone who allow their accounts to be misused by another user are liable to the same punishment.

#### **Penalties**

- i. Instances of misuse will be reported to the appropriate authorities and will lead to loss of Internet or computer privileges. Continued or repeated offences will lead to suspension or expulsion or warning.

#### **Authorized for Internet for official purpose**

- i. Managing Director (MD) and Deputy Managing Director (DMD) are authorized to keep one Broadband/DSL/4G Wireless High Speed Internet Connection including device & installation charges.
- ii. Directorate of IT at Head Office will keep two Broadband/DSL internet connections for Call Center, locally hosted online applications or managing DR site and second for usage of online applications, web-browsing, e-mail access by end-users of PBM, whereas IT Branch at PO/RO may keep one broadband/DSL internet connections.
- iii. Directorate of IT will also keep one 4G wireless internet connection as a backup to the Broadband/DSL in case of any malfunction of the same and for presentations at remote location, whereas IT Branch at PO/RO will also keep one 4G wireless internet connection for the same purpose.
- iv. Keep in view the automation of Projects/Schemes, WECs/SRCLs/DuEs/Panahgahs, PBM desks in hospitals, District offices and any new project/scheme are allowed to use one official internet connection (Broadband/DSL/4G Wireless) within the office telephone ceiling or the suitable package (maximum 100 GB data volume per month) offered by the internet service.
- v. The installation / configuration charges will be in addition to above limit.
- vi. In case of non-availability of telephone connection, wireless 4 GB connection with maximum 60 GB data volume per month is allowed.
- vii. The said expense including installation/configuration/device charges will be met out of Admin/Projects Budget of the respective office.
- viii. No other official is allowed to keep any Internet official connection.

## 24. Quality Control Policy for Data Entry

Data entry is very specialized job. As data is very important for decision making, so quality of data entry must be ensured.

Following guidelines must be followed to keep data entry as per requirement;

- i. MANUAL NOTING, INQUIRY LETTER, INTIMATION LETTER WILL NOT BE ACCEPTABLE;
- ii. All IFA cases should be processed completely through MIS software;
- iii. Concerned Branches (IFA, Projects etc) are responsible to check correctness/validity of data entry of all fields in MIS i.e. Name, CNIC, DOB, district, IFA project, disease, degree, etc) ;
- iv. All attached documents must be carefully checked before uploading;
- v. After issuance of cheque, change in Name, CNIC & District will not be accepted without approval of competent authority;
- vi. Before editing permissible fields in MIS, IT personel must cross check through documents and approval of concerned branch incharge;
- vii. All relevant staff must sign confidentiality statement and send to IT Directorate, Head Office;
- viii. In case of posting/transfer of staff, user MIS login must be disabled by concerned AD-IT upon the directions of concerned Branch incharge;
- ix. All users are responsible for the safety of their login/password;
- x. AD (IT) will give complete training to MIS users;
- xi. For any change in flow/policy/noting/letters etc, Branch Incharge will convey to IT Branch with approval of competent authority;
- xii. AD (Accounts) should not sign the cheque before its entry in MIS;
- xiii. AD (IT)/DPS should generate monthly report from software to reconcile it with Accounts Branch;

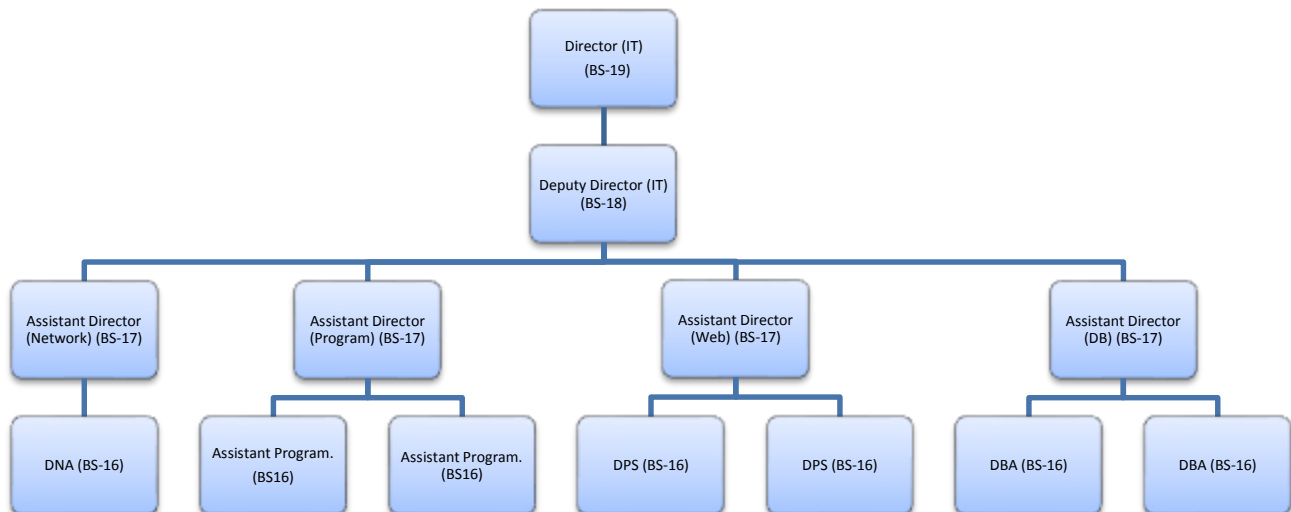
## 25. Operating Procedure - Directorate of IT

Each technical resource will perform his duties as per the Job Description (JD) issued by the Establishment Branch of PBM.

The main focus of the IT as a functional department is on providing the technological services and support to the organization by optimum utilization of available resources.

- i. Network management and troubleshooting
- ii. Management Information System (MIS) Support
- iii. MIS and Database Backup
- iv. Managing hardware resources
- v. Procurement of IT Equipment
- vi. IT Training of PBM Employees

The existing organogram is as under and Directorate of IT will propose the career path/time scale for promotion/up-gradation, keeping in view the expansion of IT infrastructure & automation of various projects/scheme. Any enhancement or change will be made with consultation of Directorate of IT.



## **26. Equipment Procurement Procedure**

This document is to serve as a set of guidelines for all PBM offices who choose to order computing equipment.

- i. One officer from IT Directorate will also be the member of technical & inspection committee for the procurement of IT equipment at PO/RO level through tender.
- ii. Procurement will be made as per PBM/PPRA rules.
- iii. Approval for the purchase of IT equipment will be routed through the IT Department, Head Office.

NOTE: All technology orders must be received by the IT Department before it can be released to the purchaser. This is to ensure that the proper software is installed and all equipment is properly tagged and placed in inventory.

### **Up-gradation of hardware**

- i. Up-gradation of IT hardware can be carried out with the approval of competent authority;

### **Condemnation**

- i. If hardware is declared out-of-order/outdated by the recommendation of Condemnation Committee/Hardware Engineer, it will be handed over to Admin Branch for auction.



## **27. Incident Management Procedure**

This procedure addresses how incidents should be handled when related to technology. This includes thefts, application/data corruption, etc.

- i. Determine scope of incident.
- ii. Fill out attached Incident Management Form.
- iii. Ensure supervisor of employee that reported or caused incident has been notified.
- iv. Submit form to Directorate of IT for onward submission to management.
- v. Administration will be notified of incident.
- vi. Resolution will be drafted given incident scope and individuals involved.
- vii. Committee will be constituted by the approval of the management for the decision regarding the incident.

## 28. Software Security and Managing Information System Policy

### Software Security

Software security is another key factor which contributes a lot in maintaining secured environments for any data processing activity. All the officers concerned must recommend suitable security classification and instructions for their programs. In order to reap the full potentials of built-in system security provisions and available software facilities for the application programs, the following may be enforced and observed regularly by the officer concerned:-

- i. Every Computer Programmer/ Data Entry Operator working on the machine may have his/her unique directory and access to it controlled by a password, known to him/her only.
- ii. Access permission to other user directories may be allowed by the concerned officer to individual Programmer/Incharge Computer/users after consulting head of the set-up and it may be strictly on "need to know basis" built-in hierarchical access path may be observed.
- iii. The packages/software provided by the IT Directorate, if any may not be changed/alterd without prior permission of Head of the IT Directorate.
- iv. Any software/package will not be deleted or installed without prior permission of Director IT.
- v. Antivirus must be installed to protect computers and data from harmful viruses.
- vi. Hardware/software firewall must be installed for protection from spyware and phishing attacks.
- vii. Firewall/proxy server log must be monitored.

### MIS & DATABASE DEVELOPMENT AND DEPLOYMENT

Development of database software is essential in supporting projects execution and also needed for digitization and data access. Following points may be considered for MIS development and deployment -

- i. MIS system shall be developed on the basis of requirements and process flows of the PBM projects.
- ii. MIS shall also be upgraded, keeping in view the new process involved in projects and for the enhancement of existing features.
- iii. MIS and database shall be developed in accordance with current available resources and strength of development team.
- iv. To keep MIS up and running. It is recommended to deploy MIS on multiple sites. Primary and secondary sites/location will be defined as PBM Data centre, NTC data centre or Nayatel server environment.
- v. Development of database software is essential in supporting projects execution and also needed for digitization and data access. Following points may be considered for MIS development and deployment
- vi. PBM's MIS/web-portals must be accessed through Secure Socket Layer (SSL) protocol to ensure security.
- vii. Backup of database and MIS should be maintained on daily basis and it should be saved in protected and on multi-places.

## Terms and Definitions

### **Appropriate Measures**

Refers to the measures that the PBM IT Department is authorized to take to secure PBM's computing resources. This may refer to measures concerning PBM owned hardware or software, data, employees, associates/visitors, etc. The PBM IT Department must maintain an appropriate measures option so that PBM is protected, concerning both equipment and information.

### **Approved Electronic File Transmission Methods**

Includes supported FTP clients including, but not limited to, FileZilla, SecureFTP, and SmartFTP. This also includes supported Web browsers including, but not limited to, Microsoft Internet Explorer, Mozilla Firefox, Netscape Navigator, and Opera. If someone have a work need to use other software/app then he/she will contact the PBM IT Department prior to use or implementation.

### **Approved Electronic Mail**

Includes all mail systems supported by the PBM IT Department. This includes, but is not limited to, PBM Webmail, Outlook configured email, and configured email on mobile devices. If you have a business need to use other mailers / application then contact the PBM IT Department prior to use or implementation.

### **Asymmetric Cryptosystem**

A method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (e.g., public-key encryption).

### **Chain email or letter**

An email sent to successive people. Typically the body of the note has direction to send out multiple copies of the note and promises good luck and/or money if the directions are followed.

### **Information System Resources**

Information System Resources include, but are not limited to, all computers, peripherals, data, and programs residing on the PBM Campuses, networks, servers, etc. These resources also include all paper information and any information for internal use only and above.

### **Information Technology Systems**

The technology department responsible for managing PBM's computing resources.

### **Configuration of PBM-to-Third Party Connections**

Connections shall be set up to allow third parties requiring access to the PBM campuses, networks, data, etc. These connections will be setup in order to allow minimum access so that third-party

entities will only see what they need to see, nothing more. This involves setting up access, applications, and network configurations to allow access to only what is necessary.

### **Domain Name System**

Essentially serves as the Internet “phone book” by associating various domain names (i.e. <http://www.pbm.gov.pk>) with their counterpart IP addresses that the computers and networking equipment need to transmit data.

### **Email**

The electronic transmission of information through a mail protocol such as SMTP, IMAP, or Exchange. Typical email clients include Mozilla Thunderbird and Microsoft Outlook.

### **Encryption**

This refers to the modification and storage of data by manipulating the way it is stored through the use of an algorithm. An encryption key is required to gain access to the original data and therefore provides the security desired.

### **Encryption Key**

A software key used to gain access to encrypted data.

### **Expunge**

To reliably erase or remove data on a PC or Mac you must use a separate program to overwrite data. Otherwise, the PC or Mac's normal erasure routine keeps the data intact until overwritten which may allow the PC to actually retain the “deleted” information for some time after the deletion took place.

### **Forwarded email**

Email received from one sender and then sent to another recipient.

### **Individual Access Controls**

Methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. This includes the utilization of passwords, screensavers, hardware encryption, etc.

### **Insecure Internet Links**

All network links that originate from a locale or travel over lines that are not totally under the control of PBM. These types of connections can allow an unidentified third-party to intercept, monitor, or copy the traffic being sent across this connection.

### **Internet**

A worldwide, publicly-accessible series of interconnected networks used to transmit packets of data

via the Internet Protocol (IP).

### **Internet Protocol**

A data-oriented network protocol used to transmit data across a packet-switched network such as the Internet.

### **Local Area Network**

A computer network covering a small geographic area. These can include a single campus, a single building, or even a single room.

### **One Time Password (OTP) Authentication**

This type of authentication is accomplished by using a one-time password token to connect to a IFA E-Filing BMS over a LAN/WAN for payment disbursement.

### **Personal Computer**

A device used by a single user to access local programs and files, network resources, or the Internet. This can include desktop, laptop, tablet, or portable computers.

### **Physical Security**

Physical security refers to the actual physical security mechanisms in place to prevent unauthorized access to technology resources. This can also mean having actual possession of a computer or by locking the computer in an unusable state to an object that is immovable. Methods of accomplishing this include having a special key to unlock the computer so it can be used, thereby ensuring that the computer cannot be simply rebooted to get around the protection. If it is a laptop or other portable computer, never leave it alone in a conference room, hotel room, in a vehicle, on an airplane seat, etc. Make arrangements to lock the device in a secure location such as a hotel safe or take it with you. In the office, always use a lockdown cable. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer, cabinet, safe, etc. or simply take it with you.

### **Private Link**

An electronic communications path for which PBM has control over the entire distance. These types of links typically use a VPN tunnel or other means to connect two or more locations. For example, all PBM networks are connected via a private link.

### **Proprietary Encryption**

An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.

### **Public Link**

An electronic communications path for which PBM does not have control over the entire distance. This connection does not utilize any special connection scheme. A connection from any PBM

computer to the Internet is an example of a public link.

### **Secure Internet Links**

All network links that originate from a locale or travel over lines that are either under the control of PBM or utilize technology to form a secure “pipe” for information to traverse. These types of connections prohibit an unidentified third-party to intercept, monitor, or copy the traffic being sent across this connection by solely utilizing the PBM network or utilizing a secure authentication mechanism to connect

### **Sensitive information**

Information is considered sensitive if it can be damaging to PBM, its employees, associates, etc. This information can include personnel data, projects/schemes information, purchasing information, etc.

### **Symmetric Cryptosystem**

A method of encryption in which the same key is used for both encryption and decryption of the data.

### **Unauthorized Disclosure**

The intentional or unintentional revealing of restricted information to individuals, either internal or external to PBM, who do not have a need to know that information.

### **User Authentication (Local)**

A method by which the user of a system can be verified as a legitimate user on that system only.

### **User Authentication (Network)**

A method by which the user on a network can be verified as a legitimate user independent of the computer or operating system being used.

### **Virtual Private Network**

A network that functions as a single, secure network that is usually comprised of several locations residing in separate geographic areas. This is accomplished through the use of secure, authenticated connections from one network to another.

### **Virus Warning**

Typically, these are emails containing warnings about virus or mal-ware. The overwhelming majority of these emails turn out to be a hoax and contain bogus information usually intent only on frightening or misleading users. However, the PBM IT Department occasionally sends out virus warning should the need arise. In these cases, recipients should heed the warnings provided by the IT Department employees rather than treat the information as potentially misleading.

### **Wide Area Network**

A computer network covering a large geographic area. The Internet is an example of a WAN.

## **29.Disclaimer**

The PBM IT Department regards this document as a work in progress. Because of this, these policies and procedures undergo regular reviews and modifications. Therefore, it is up to each individual employee or associate to remain current on the updated policies and procedures.

Changes in these policies and procedures after the initial agreement signature date does not allow non-compliance or permit the employee or associate to engage in activities contradictory to the modifications made after the initial agreement signature date.

## Forms

### 30. User Create Form

Date: \_\_\_\_\_

*User/Employee requesting access:* \_\_\_\_\_

Name: \_\_\_\_\_ Designation: \_\_\_\_\_

Email Address: \_\_\_\_\_

Cell Phone: \_\_\_\_\_ Signature: \_\_\_\_\_

*Branch/Directorate making request:* \_\_\_\_\_

Name: \_\_\_\_\_ Designation: \_\_\_\_\_

Reason to Access: \_\_\_\_\_ Signature: \_\_\_\_\_

*Type of access needed:* \_\_\_\_\_

System: \_\_\_\_\_ Duration: \_\_\_\_\_

System: \_\_\_\_\_ Duration: \_\_\_\_\_

System: \_\_\_\_\_ Duration: \_\_\_\_\_

System: \_\_\_\_\_ Duration: \_\_\_\_\_

System: \_\_\_\_\_ Duration: \_\_\_\_\_

*Special Requirements:* \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_

PBM IT Department Personnel Use Only: \_\_\_\_\_

Receiving Employee: \_\_\_\_\_ Date: \_\_\_\_\_

Access Created? Yes – No – Other: \_\_\_\_\_ Date: \_\_\_\_\_

Details: \_\_\_\_\_ Signature: \_\_\_\_\_



### 31. Equipment Transfer Form

Date: \_\_\_\_\_

User receiving equipment:

Name: \_\_\_\_\_ Company: \_\_\_\_\_

Cell Phone: \_\_\_\_\_

Signature: \_\_\_\_\_

Employee transferring equipment:

Name: \_\_\_\_\_ Designation: \_\_\_\_\_

Office: \_\_\_\_\_

Signature: \_\_\_\_\_

Equipment being transferred:

Item 1: \_\_\_\_\_ Serial #: \_\_\_\_\_ PBM #: \_\_\_\_\_

Item 2: \_\_\_\_\_ Serial #: \_\_\_\_\_ PBM #: \_\_\_\_\_

Item 3: \_\_\_\_\_ Serial #: \_\_\_\_\_ PBM #: \_\_\_\_\_

Item 4: \_\_\_\_\_ Serial #: \_\_\_\_\_ PBM #: \_\_\_\_\_

Item 5: \_\_\_\_\_ Serial #: \_\_\_\_\_ PBM #: \_\_\_\_\_

Item 6: \_\_\_\_\_ Serial #: \_\_\_\_\_ PBM #: \_\_\_\_\_

Item 7: \_\_\_\_\_ Serial #: \_\_\_\_\_ PBM #: \_\_\_\_\_

Item 8: \_\_\_\_\_ Serial #: \_\_\_\_\_ PBM #: \_\_\_\_\_

Special Requirements/Notes:

\_\_\_\_\_

PBM IT Department Personnel Use Only:

Receiving Employee: \_\_\_\_\_ Date Received: \_\_\_\_\_

Details: \_\_\_\_\_

## 32. Incident Report Form

Date: \_\_\_\_\_

User Causing/Experiencing Incident: \_\_\_\_\_

Name: \_\_\_\_\_ Designation: \_\_\_\_\_

Cell Phone: \_\_\_\_\_ Office: \_\_\_\_\_

Incident Title: \_\_\_\_\_

Incident Details: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

Special Requirements/Notes: \_\_\_\_\_

\_\_\_\_\_

Signature: \_\_\_\_\_

PBM IT Department Personnel Use Only: \_\_\_\_\_

Receiving Employee: \_\_\_\_\_ Date Received: \_\_\_\_\_

Details: \_\_\_\_\_

\_\_\_\_\_

Additional Steps Needed: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

### 33.DATA ACQUISITION FORM

Name of Officer: \_\_\_\_\_ Designation: \_\_\_\_\_

Branch: \_\_\_\_\_ Date: \_\_\_\_\_

Detail of data required: \_\_\_\_\_

Purpose of data: \_\_\_\_\_

Format of report: Print / Excel / PDF

Data fields required in report:

\_\_\_\_\_  
Signature of Director / Branch Incharge

Request examined & approved by :

\_\_\_\_\_  
Director (IT)

### 34.Handing Over /Taking Over

#### Receipt

S.No.	Item	Quantity
-------	------	----------

1.

Note:-

The above mentioned item at serial No.1 is in working condition and above said item shall not move or transfer to any other branch without written permission of IT Directorate.

Handing Over

Taking Over

Name:-\_\_\_\_\_

Data Network Administrator

Designation:-\_\_\_\_\_

IT Directorate

Section\_\_\_\_\_

\_\_\_\_\_  
Director (IT)

### **35.Policies and Procedures Manual Compliance**

The forms following this page are required for every employee upon successfully reading and agreeing to the policies and procedures set forth within this document. All other forms mentioned earlier within this document may be used as needed during daily activities and as required for performing job duties.

A copy of these two forms shall be retained by the PBM IT Department to ensure all employees have signed and agreed to the policies and procedures included herein.

An employee's signature on a previous version of this policies and procedures manual does not exclude any user from being required to abide by any new or updated policies or procedures. Any signature, by any employee, upon first being hired is transferable to subsequent iterations of this document from henceforth so that all current employees shall not be required to re-sign these documents.

Upon successful approval of changes, a copy shall be made available for all employees so that any current employee may view new policies and procedures and/or any changes to current policies and procedures.

Employees may obtain a current copy of this document from the PBM IT department at any time.

### 36.Non-Disclosure Agreement Form / Confidentiality Statement (For IT Personnel)

I certify, by signing below, that I have read and understand my responsibilities for the usage of IT resources. Also, by signing below, I agree to abide by the aforementioned agreement/statement having known and understood the consequences outlined above.

Date: \_\_\_\_\_

Name: \_\_\_\_\_ Designation: \_\_\_\_\_

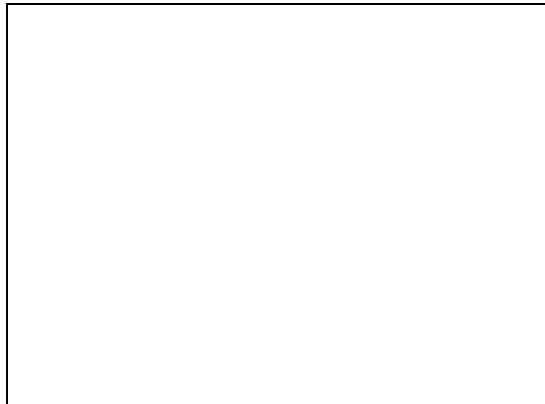
Office: \_\_\_\_\_

Signature: \_\_\_\_\_

### 37. Authorization/Confidentiality Statement (For personnel using IFA e-filing BMS)

#### **AUTHORIZATION / CONFIDENTIALITY STATEMENT**

I hereby authorize to insert my electronic signature in E-Filing BMS to process / recommend IFA cases. From now onwards, I shall be responsible for my own login & password and keep it confidential.



Name : \_\_\_\_\_

Designation : \_\_\_\_\_

Branch : \_\_\_\_\_

Date : \_\_\_\_\_

This issues with the approval of Bait-ul-Mal Board its 70<sup>th</sup> meeting held  
on 2<sup>nd</sup> April, 2021

Signed by

---

**Director (IT)**

Counter Signed by

---

**Director (Admin)**