Information Technology (IT) Policy

THE PUNJAB STATE COOPERATIVE AGRICULTURAL DEVELOPMENT BANK Ltd.

SCO – 53-54, SECTOR 17B, BANK SQUARE, CHANDIGARH.

Version 1.0 (01-08-2024)

Contents

1. Introduction

Punjab State Cooperative Agricultural Development Bank Ltd. (PSCADB) provides 'IT Resources' to its employees for official use to support the enhancement of a quality learning environment and to improve productivity and efficiency in management & administration. These resources are meant as tools to access and process information related to their areas of work. These resources assist them to remain well informed and carry out their functions in an efficient and effective manner.

This Information Technology (IT) Policy of the Bank defines rules, regulations and guidelines (issued separately) for proper usage and maintenance of these IT Resources to ensure their ethical, acceptable and legitimate use and to assure protection, safety and security of data, products, facilities as well as the people using them.

Since this is a common policy document, it is generic in nature and therefore does not provide technical recommendations or procedures. Instead, this document describes what the policies are, why they have been set and what the consequences of failing to comply with the policy are. This document acts as an umbrella over all other departmental or office policies relating to computer and information security and provides a benchmark for measuring their compliance and alignment.

It applies to all employees of and contractors to Bank and to any individual, or organization which the Bank permits the access to its Computer Network (in this policy referred to collectively as "Users").

Employees of the Bank are expected to report suspected breaches of this policy, and any unacceptable behavior which occur in the Bank by a person acting in his/her capacity as an employee of the Bank, the report should be directed to the Managing Director of the Bank and will be treated in a confidential and responsible manner. The Bank will protect the interest of any of its official or employee reporting a suspected breach in good faith and in a responsible way.

2. Definitions used in this policy

Please read Appendix A - Definitions.

3. Responsibilities

Every user is responsible for safeguarding the IT Resources of the Bank and the information contained therein. Every user is also responsible for using Bank's IT Resources and information in an effective, ethical, and lawful manner and to comply with this policy at all times.

a. Users' Responsibilities

If a potential security breach is observed, reasonable and appropriate measures should be taken to address it.

"Users must take all reasonable care in their actions and work practices to ensure that Information is kept secure at all times. Users are also responsible for taking appropriate and reasonable actions to secure any part of the IT Resources or Information observed to be at risk, whether or not they have direct responsibility for those resources."

4. Compliance and Disciplinary Action

The Bank takes security of its IT Resources and information contained therein, very seriously. This policy document has been created to protect the Bank's interests by protecting the IT Resources, and its use. Any non-compliance with this policy, therefore, will be viewed seriously and as a direct threat to the Bank's interests. The Bank will respond with any or all means at its disposal to counter such threats to its interests.

The consequences for users who do not comply with this policy can be severe.

- If a user is a Bank employee, a breach of this policy could result in disciplinary action– including dismissal in appropriate cases.
- If a user is a contractor to, or an organization engaged to provide services to the Bank, a breach of this policy could result in the Bank having a right to seek damages against the contractor / organization, and / or blacklist the contractor / organization, and / or it being able to terminate the contractor / organization's contract, depending on the actual terms of the contract.

5. Policy Scope

This policy describes standards and procedures that reflect safe and acceptable practice based on accepted and current knowledge, guidelines and common practice. The Bank will create the necessary measures and assign responsibilities to protect Information from loss, theft, and unauthorized modification, disclosure or unauthorized access.

These measures shall apply to all the Bank owned information and all the information for which Bank is otherwise responsible, either physical or electronic. All users must comply with these security measures.

All the users who use the IT Resources or information come under the purview of this policy and will have to abide by the regulations / directions / guidelines of the policy.

6. Interpretation, Changing and Relaxation

The power of interpreting, changing and relaxing of policy instructions is vested with the Managing Director of the Bank.

"Power of any amendment / change / relaxation in this IT Policy is vested with the Managing Director of the Bank."

7. Governing Policy

a. Information Proprietary Rights

The Bank has a substantial investment in its IT Resources. In the interest of the security of that Network and Information, it is important to be very clear about its ownership and how it may be accessed and used.

> ***"The IT Resources, and the information it stores, generates, or which is transmitted over the computer network, are the exclusive property of the Bank (unless Bank agrees otherwise with the provider of the Information). This information may only be accessed and used exclusively for the support of Bank's interests, except as allowed for by section 6".***

This does not include the use of rental or lease equipment where the ownership of the physical asset may remain with another company. However, any Information or configuration stored on such assets remains the property of the Bank.

> ***"Any information stored on rental or lease equipment must be irrecoverably removed from equipment no longer owned by or in the control of the Bank, before ownership or possession of the equipment passes to another party*.**"

b. Individual Rights and Responsibilities and "Acceptable Use"

The Bank is committed to protect its employees, partners and the institution from illegal or damaging actions by individuals or group of persons or firms etc, either knowingly or unknowingly. Internet / Intranet - related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, internet browsing, and FTP, are the property of the Bank. These systems are to be used for business purposes in serving Bank's interests, and those of its subsidiaries and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every employee who deals with information and / or IT Resources. It is the responsibility of every user to know these guidelines, and to conduct their activities accordingly.

Bank's information may only be accessed and used exclusively for supporting the interests of the institution. Private use or un-authorized disclosure of the Bank's information is strictly prohibited.

The Bank's IT Resources should primarily only be accessed and used exclusively for supporting the interests of the institution. Incidental personal use of the IT Resources is permitted, provided it does not consume more than a trivial number of resources, does not interfere with productivity or the business functions and complies with the other rules set out in the Bank's policies (including rules as to illegal and inappropriate use).

Using the institution's IT Resources for any purpose – whether business or personal - automatically grants the Bank, the right to actively monitor and audit the usage to protect its interests.

Acceptable Use -

1. While the Bank's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the computer systems remains the property of the Bank. Because of the need to protect Bank's network, management cannot guarantee the confidentiality of information stored on any network device not belonging to the Bank.

2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet / Intranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their Branch Manager / Incharge.

3. For security and network maintenance purposes, authorized individuals within the Bank (IT Officials etc.) may monitor equipment, systems and network traffic at any time.

4. Bank reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and Proprietary Information

1. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed at least once in every six months, user level passwords should be changed at least once in a month. These passwords must be kept secured and should not be shared.

2. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Windows users) when the system remains unattended.

3. Because information contained on portable computers is especially vulnerable, special care should be exercised.

4. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, Trojan horse code or ransomware code.

5. Information held on the Bank's computer network – whether business-related or for a user's private use – may be made available to the Police and/or other appropriate authorities at the Bank's discretion;

6. The use of the Computer Network automatically grants the Bank full rights to access any resulting files and information and, at the Bank's discretion, ownership of those files and that information.

Unacceptable Use

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 (officials of Computer Cell posted either at Head Office or in the field) may have a need to disable the network access of a host if the host is virus infected).

Under no circumstances is an employee of Bank authorized to engage in any activity that is illegal under local, state, or national law, while utilizing Bank's-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.

System and Network Activities

The following activities are strictly prohibited.

a) It is always inappropriate and can be unlawful to use the Bank's IT Resources to import, store, view or distribute offensive, objectionable or illegal material;

b) 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 in the Bank.

c) 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 the Bank or the end user does not have an active license is strictly prohibited.

d) Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal.

e) Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

f) Revealing your account password to others or allowing use of your account by others. Exceptions to the above include, revealing account password to the IT Officials / System personnel, for troubleshooting / detecting the software deficiency.

g) Using a Bank's 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.

h) Providing information about, or lists of, Bank employees to external parties/ agencies/ institutions.

i) Installation of any software on Bank's computers without first consulting Computer Cell official. This includes any software downloaded from the internet as well as any personal software brought in from other sources. Installing any unauthorized software can in turn create problems with the functioning of the computer and/or the software installed on it.

j) 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.

Email and Communications Activities

a) 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).

b) Creating or forwarding "chain letters".

c) Posting the same or similar non-business-related messages to large numbers of newsgroups (newsgroup spam).

c. Use of Disclaimers for Electronic Communications Channels

Communicating externally using the Bank's computer network, such as e-mail, posting from Bank's Social Media Channels, implies that the content of the e-mail/ post is the official view of the Bank.

"Any unofficial external communications, making use of Bank's official electronic communications channels like E-Mail, Social Media etc., must include an approved disclaimer."

d. Information Disposal

The life cycle of storage hardware is relatively short. Escalating demands for capacity is a significant factor in this. An inevitable result is the growing requirement to reuse, or dispose of media once used to store classified information.

"Any media containing classified information which is no longer required must be disposed of in a secure manner."

Storage media may include Paper, Floppy disk, CD-ROM, DVD, Magnetic Tape, Pen Drive, HDD, SSD etc. and appropriate disposal mechanisms would include shredding and secure waste bins.

8. Resource Usage and Access

When a user uses the Bank's computer network, both the physical network, and the contained information, may be accessed and used. These resources are secured during three main types of activities:

- User profile is a template of what parts of the computer network, and what information, an individual user has the authority to access and use. In the developed Application Software, every User has a profile unique to them, which is applied system-wide regardless of how the systems are accessed;
- User Authentication is a mechanism of ensuring that the person accessing the Computer Network and information made available through a user profile, is the legitimate user, the profile was created for.
- It is important to distinguish between the Administrative User and a General User, for the purposes of auditing and minimising the number of people with high-level privileges. A user who has the ability to perform administrative functions should not be using the administrative account for day-to-day usage – they will also have a general account which must be used in those circumstances; and

- "Communications" refers to the way in which a user connects to the computer network. Different security measures can be applied to the communication mechanism depending on what mechanism is chosen. Securities are applied to ensure that only the authenticated user can view information, or use the computer network over the communications mechanism.

"Access to and use of the Bank's computer network will be secured through a combination of authorised unique User profiles, authenticated User access and applied security measures appropriate to the communication mechanism.".

a. Network Access

Passwords are generally the last security barrier before a potential intruder gains access to the computer network. Because passwords are linked with user account names, they also validate an audit of user's actions whilst logged in under their user account name. Keeping network access details confidential is therefore essential.

Shared User accounts defeat the principle of accountability, which attempts to attribute all system events to specific individuals.

"All user accounts must be unique to each individual user of the Bank Computer Network. User accounts contain the user's profile."

"Access to the Bank's computer network via shared user accounts is prohibited."

Refer to **Appendix B** for specific policies regarding passwords. Users are responsible for taking all reasonable precautions to ensure any material they introduce to the computer network is suitable for the Bank's business use.

Special care is required when the information is being used on equipment not owned by the Bank. Because the equipment is out of the direct control of the Bank security mechanism, the Users using that information are responsible for taking all reasonable steps to protect the information's integrity and preventing unauthorized access to it. All requirements of this policy must be applied to the use of that equipment.

9. Access to Information

An individual user's access to information is a function of the role they perform for the Bank. Access rights must be controlled and appropriate according to the user's current role. As a user's role changes or the user no longer performs a role for the Bank, the concerned Branch Head/Manager should immediately inform the Computer Cell.

"Access rights must be controlled to ensure that they are appropriate for each user's current role."

"Responsibility for providing access control lies with the System Administrator."

10. External Access

a. Network Scope

Many major security risks can be averted if access to the Bank's computer network remains secure from unauthorised external access by being confined within its boundaries.

Boundaries represent a double risk to the Bank because they provide a potential exit point for the unauthorised escape of information from the Bank's computer network and an entry point for compromising the integrity and availability of the Bank's information. This includes computer viruses, malicious damage and unauthorised access to, or use of, the Bank's computer network.

"All the boundaries of the Bank's computer network must be secured against un-authorised access."

b. Remote Access

The most effective way to secure a boundary is to remove any external access to it. However, removing all external access is not a viable option for the Bank as there are many valid requirements for such access.

Points of access therefore are permissible but only if they are able to -

(i) authenticate and allow access for third party support and
(ii) authenticate and allow access for legitimate Users and deny all other access.

The very existence of networks creates a security risk for the Bank, given that their purpose is to access, share and move information. Fundamental to the success of any efficient, secure and well-run network is centralized design and management.

"The design, control and management responsibilities for all networks within the Bank will be centralised under System Administrator of the Bank."

c. Third Party Access

Third parties will be granted remote access into the Bank's network only if they require it to perform maintenance, troubleshooting, upgrades or monitoring of systems they have provided to the Bank. Access will be limited to the specific server/machine and communication port (TCP/IP) which are the minimum necessary to perform the required support.

Upon termination of the process, contract/agreement with the Bank, remote access to third party will be terminated and any Bank provided equipment will be returned.

d. Virus Detection

Any data received from an external source has a degree of risk associated with it such as introducing viruses or malicious code. To guard against this, virus detection is built into any external access mechanism. Responsibility for purchasing and installing/updating the protection mechanisms for

viruses lies with head of the Computer Branch. Users must ensure data from an external source is scanned for viruses before introducing it to the Bank's computer network.

"Any data introduced to the Bank's Computer Network from an external source must be screened for the presence of malicious code (including viruses)."

11. Business Continuity

All users must ensure that any IT resources that are required in the course of their work are adequately covered by a backup plan.

a. Business and Computer Continuity Planning Process

This policy requires that a formal process exists for the preparation and maintenance of the computer and Information Technology Service Continuity Plans.

Nodal Officer shall be responsible for maintaining the **Disaster Recovery Plan (DRP)** for the institution.

b. Preparation and Maintenance of Computer Emergency Response Plans

Emergencies require immediate attention but may not have long-term implications or serious financial consequences. Disasters have long-term implications, have serious financial consequences, and may or may not require immediate attention.

Nodal Officer shall be responsible for maintaining the **Computer Emergency Response Plan (CERP)** for the institution.

c. Backing Up of Critical Data

The intention of this policy is to specify a minimum acceptable backup timeframe and also to specify what type of information needs to be backed-up. Certain types of information will need to be backed up more frequently, but these decisions must be made on an organisational and information type basis. These decisions should also be reviewed regularly as the critical back-up requirements may change over time.

Nodal Officer will be responsible for developing/maintaining a schedule for backing up the computer systems depending upon configuration, software applications, nature of data and other factors. This schedule must be documented and made available to users for references. Nodal Office will also ensure these procedures are followed strictly and implemented as per rules.

Bank's branches will ensure that the computer system available for data backup as per the approved planned schedule handed to them. Remote Backup Services could also be taken for backup and recover important data on the Local Area Network (LAN).

Computer Cell of the Bank shall maintain backup infrastructure, including upgrading the hardware and software as needed.

"All critical business information and critical software resident on the Bank's Computer Systems must be periodically (as per backup schedule) backed-up. These backup processes must be performed with sufficient frequency. "

Backup Process

"The purpose of backup is to protect the files on the Computer System's Hard Disks from catastrophic loss. The backup of disk files is performed on a daily basis to protect data from being lost due to a hardware or software malfunction. "

Recommendations on Backup of Applications and Documents

For Individual Desktop

Backup should be taken on removable storage media or devices such as Zip drives, CD-ROM, Flash Drives etc. Appropriate backup software can also be used for taking regular backups.

The General Branch of the Bank is responsible for purchasing removable media (e.g. CDs, DVDs, Pen Drives, Zip disks, etc) and distributing the same on demand to the branches.

In case of lost or damaged system files and standard applications, user is required to immediately inform the System administrator/IT Nodal Officer for solution.

To ensure the safety of backup files, users should:

- Keep one copy of backup data with them under lock and key. The other copy of backup data shall be kept with the Computer Cell of the Bank, for restoration purpose.
- Keep documents in an appropriate folder and assign similar short names for easy backup.
- Back up entire Documents/ folder to the removable media at least once a week or daily if documents are frequently created/changed.
- Maintain at least 2 backup sets, alternating their use. Thus, if latest backup goes bad, there will still be the other backup of older version.

For Network Users

Users Working on the customized Application Software will be allocated a separate account for interacting with different modules. Allocation of modules shall depend on the branch of the user and the job which the user is required to perform in the branch. Since different users within the branch are required to perform different jobs, similarly, different privileges/ permissions are allocated to users on basis of jobs being performed by them.

Off-site Storage

In order to provide disaster recovery capability, backup CDs/DVDs should be backed up to a secure off-site storage facility.

d. Regular Testing of Stored Data Media

The intention of this policy is to ensure that archival information will be readily recoverable if and when it is needed.

"Critical business information and critical software on computer storage media for a prolonged period of time must be tested periodically (at least once in six months) to ensure that the Information is still recoverable."

e. Off Site Storage of Backup Media

This policy ensures that backups are protected from local environmental disasters.

"Backups of essential business information and software must be stored in an environmentally-protected and access-controlled site which is a sufficient distance away from the originating facility to escape a local disaster."

12. Hardware

a. Primary User

An official in whose room or on whose table, the computer is installed and is primarily used by him/her, shall be considered as "Primary" user. Where a computer system has multiple users, none of whom are considered the "Primary" user, the Manager of the Branch where the computer system has been installed shall make an arrangement and make an official responsible for compliance.

b. Hardware Inventory

To secure the hardware assets, an accurate inventory (the Fixed Asset Register), which includes the location of all hardware, shall be kept. The purpose of this inventory is to ensure that all hardware is accounted for, physically and financially. The Fixed Asset Register shall be maintained by the Computer Branch.

"An accurate inventory of hardware must be maintained and reconciled annually with the Computer Branch's Fixed Asset Register."

c. Hardware Responsibility

To protect the Bank's investment in hardware, primary users are responsible for taking all reasonable steps to protect hardware from damage or loss. Special care is required when any part of the IT resource is removed from the Bank's premises. In removing any of the IT resources from the limits of the Bank's premises, individuals must take all reasonable steps to ensure the resource's physical security.

"All care must be exercised to ensure Computer Network hardware is not subjected to conditions, circumstances or acts that may cause damage or loss."

d. Hardware Physical Security

Particular care must be taken to ensure the physical security of mission critical hardware (Servers, Switches etc.) since the impact of its damage or loss is greater than other hardware.

"Mission critical hardware must be securely housed and appropriate physical access restrictions applied."

e. Authorized Hardware Changes

Hardware that is incorrectly repaired or configured or is configured without paying due care to appropriate work practices, can cease to function and can pose a threat to the function and integrity of other hardware, software and data. It is therefore important that only appropriately skilled and authorized people (Computer Cell officials) work on hardware configuration/ maintenance etc.

"Hardware may only be installed, configured, modified, repaired, or uninstalled by appropriately skilled and authorized personnel in accordance with a documented change control procedure."

f. Hardware Deployment

Because the Bank's computer network resources are deployed exclusively to support its business requirements, a strategy for deployment must exist to ensure optimum balance of efficiency, effectiveness and responsiveness. To preserve the integrity of the strategy, hardware can only be acquired after the appropriate expenditure and management approvals have been given.

"There must be adequate controls over the procurement of hardware to ensure purchases comply with the deployment strategy and are appropriately authorized."

g. Hardware Malfunction

The most common cause of data loss, hardware malfunction or hard drive failure, is another necessary evil inherent to computer functioning. There is usually no warning that hard drive will fail, but some steps can be taken to minimize the need for data recovery from a hard drive failure:

- if system runs the scan disk on every reboot, it shows that system is carrying high risk for future data loss. Back it up while it is still running.
- if system makes any irregular noises such as clicking or ticking coming from the drive. Shut the system down and call the Computer Cell official / Hardware Engineer for more information.
- use an UPS (Uninterruptible Power Supply) to lessen malfunction caused by power surges.
- keep the computer away from heat sources and make sure it is well ventilated.
- never open the casing on a hard drive. Dust settling on the platters in the interior of the drive can cause it to fail.

h. Hardware Purchase

The purchase of new computers and peripherals requires careful consideration of operations needs because it is usually expensive to make subsequent changes.

In order to ensure transparency in the purchase of Computer Hardware and Peripherals for the Head Office, purchases will be done by the Computer Hardware Committee constituted by the Board of

Directors of the Bank through any of the methods defined in the "The Punjab Transparency in Public Procurement Act 2019 and Rules 2022" as amended from time to time.

Members in the present Computer Hardware Committee are as under:

a. Chairman of the Board of Directors of the Bank (Chairman)
b. Managing Director of the Bank
c. Two members from Board of Directors
d. In-charge Computer Cell (Convener) of the Bank

The above Committee shall meet as and when the need arises for the purchase of Computer Hardware / Software.

In order to keep standardization of Computer Hardware / Software in the field, Primary Banks, having independent Managing Committees are bound to make purchases of Computer Hardware / Software based on specifications / configurations recommended by the Head Office. For the purpose, they can form committee comprising of the following officials:

a. Manager of the Primary Bank
b. District ITO (Technical official)
c. Audit Inspector of the Bank

"All purchases of new Computer Systems (Desktop / Laptop / Server etc.) shall be made in accordance with the decision of the Computer Hardware Committee of the Bank through any of the methods defined in the "The Punjab Transparency in Public Procurement Act 2019 and Rules 2022" as amended from time to time".

"All purchases of add-on peripherals required for installation with the Computer Systems (whether new or old) shall be done with the approval of the Managing Director of the Bank".

i. Hardware Maintenance

As far as possible, the Bank shall procure new Hardware which is covered under 3-5 years Service Warranty. On the expiry of the above period and in order to have trained hands, the Bank shall sign an "Annual Maintenance Contract / Agreement" with the approved Hardware Vendor selected by way of Closed Quotation / Open Tender, as the case may be. Where the life of equipment / computer / peripheral has surpassed the approved tenure and to keep the equipment running, the maintenance shall be got done from Hardware Vendors, on per call basis.

All the computers and peripherals should be strictly connected to the specially provided electrical points through UPS. Power supply to the UPS should never be switched off, as continuous power supply to UPS is required for battery recharging, till such instances wherein the UPS is to be left unattended. Further, these UPS systems should be connected to the electrical points that are provided with proper earthling and have properly laid electrical wiring. Responsibility of continuous power supply, proper earthing and properly laid electrical wiring lies with the General Branch.

"In order to secure Bank's IT Resources, all the new computer systems (laptop / desktop / server etc.) purchased by Bank should be covered under 3 – 5 years of warranty period".

"For the safety & security of the Bank's IT Resources and where the life of the equipment is within the approved tenure (3-5 years), Annual Maintenance Contract shall be signed with the authorized Hardware Vendor, after the expiry of the warranty period."

13. Software

a. Software Inventory

To secure these assets, an accurate inventory, which includes the licenses and installed instances of all software, must be kept. The purpose of this inventory is to ensure that all software can be accounted for physically and financially.

"An accurate inventory of software licenses and instances must be maintained and reconciled annually by the Computer Cell of the Bank."

b. Installation Media

Access to the original software installation media should be restricted to those with responsibility for installing it, should re-installation be required.

"Software installation media containing mission critical software must be stored securely to prevent loss or corruption."

c. Unlicensed Software

Software is not always purchased. It can be proprietary, meaning it has been developed and used for a specific requirement by the owner, or it is licensed, meaning a license can be obtained from the developer to use the software but ownership remains with the developer. Using unlicensed non-proprietary software can expose the Bank's and individual users to significant claims of breach of copyright. Such software is also unsupported by the vendor and endangers the integrity of the Bank's other software through an increased risk of instability and viruses.

Adhering to Anti-Piracy laws of the country, Bank's IT Policy does not allow any pirated / unauthorized software installation on the institution owned computers. In case of any such instances, the primary user shall specifically be responsible for any pirated software installed on his/her computer system.

"Only licensed software or software for which the Bank has proprietary rights may be used on the Bank's Computer Network."

d. Authorized Software Changes

Software that is incorrectly installed, configured, modified or uninstalled, can cease to function and can pose a threat to the function and integrity of other software, hardware, and information. It is therefore important that only appropriately skilled and authorized people work on the installation and configuration of software.

"Software may only be installed, configured, modified, repaired or uninstalled by appropriately skilled and authorized personnel in accordance with change control procedures."

e. Software Deployment and Procurement

Because the Bank's computer resources are deployed exclusively to support its business requirements, a strategy for deployment must exist to ensure the optimum balance of efficiency, effectiveness and responsiveness. To preserve the integrity of the strategy, software can only be acquired after the appropriate expenditure and management approvals have been given.

"There must be adequate controls over the procurement of software to ensure it complies with the computing resource strategy and is appropriately authorized."

f. Software Malfunction

Software malfunction is a necessary evil when using a computer. Even the world's top programs cannot anticipate every error that may occur on any given program. There are still few things that can lessen the risks:

- Be sure the software used is meant only for its intended purpose. Misusing a program may cause it to malfunction.
- Using pirated copies of a program may cause the software to malfunction, resulting in a corruption of data files.
- Be sure that the proper amount of memory installed while running multiple programs simultaneously. If a program shuts down or hangs up, data might be lost or corrupt.
- Back up is a tedious task, but it is very useful if the software gets corrupted.

g. Antivirus Software

All computer systems used in the Bank should be secured with a licensed Anti-Virus Software, and it should be active for download of latest security patches at all times. The primary user of a computer system is responsible for keeping the computer system compliant with virus protection policy.

h. Software Purchase

The purchase of new System Software (Anti-Virus Software, Operating System Software etc.) by the Bank shall be finalized following the procedure and by the Committee as defined in 12(h).

"All purchases of new Software (Operating System, Anti-Virus etc.) shall be made in accordance with the decision of the Computer Hardware Committee of the Bank through any of the methods defined in the "The Punjab Transparency in Public Procurement Act 2019 and Rules 2022" as amended from time to time".

****

Appendix A

Definitions used in this Policy

"**Acceptable Use Guidelines**" means the "Bank's General Computer, Internet and Email Guidelines", which set out the guidelines for the acceptable use of the Bank's Computer Network and Information.

"**Bank**" means The Punjab State Cooperative Agricultural Development Bank Ltd (PSCADB).

"**Computer Network**" means the Bank's computer network and includes all hardware (including portable computers), software, floppy disks, CD-ROMs, other storage media, modems, and other network resources.

"**Computer Security**" means the protection of the Bank's Computer Network from un-authorized access and/or usage, while maintaining the reliable operation of those computer networks.

"download" means the transmission of a file from one computer system to another. From the Internet user's point-of-view, to download a file is to request it from another computer (or from a Web page on another computer) and to receive it.

"Electronic Communications Channel" means any process, or mechanism that provides the ability to move electronic information from one point to another.

"email" means Electronic Mail. This includes institution email systems, web mail systems (like HotMail) and any other system that electronically transfers messages in a "store and forward" manner.

"**Information**" means any information held on or transmitted over the Bank's computer network, whether or not in printable format, and includes any file, document, electronic mail communication and where any information is printed onto paper, includes the paper version of that information.

"**Information Security"** means the preservation of the confidentiality, availability and integrity of the Bank's information, where "confidentiality" is defined as ensuring that information is accessible only to those authorized to have access, "availability" is defined as ensuring that authorized Users have access to Information and associated assets when required, and "integrity" is defined as safeguarding the accuracy and completeness of information.

"Internet" means an interconnected system of networks that connects computers around the world via the TCP/IP protocol.

"Intranet" means a privately maintained computer network that can be accessed only by authorized persons, especially members or employees of the organization that owns it.

"**IT Resources**" means

- Desktop/ Laptop/ Server
- Peripheral Devices (Printer/ Scanner/ MFD/ Keyboard/ Mouse/ Speaker/ WebCam etc)
- Network Devices (wired/wireless)
- Official Website / Web Application
- Internet Access
- Storage Devices.

"Mission Critical" means if the system, or application fails, crashes, or is otherwise unavailable to the organization, it will have a significant negative impact upon the business.

"**User**" means any authorized user of the Bank's IT Resources, and includes employees of, and contractors to, the Bank and any individual, or organization which the Bank permits the use of or access (including by connecting remotely) to the Bank's computer network.

****

Appendix B

Password Policy

- "The selection of passwords, their use and management as a primary means to control access to systems is to strictly adhere to best practice guideline. In particular, passwords shall not be shared with any other person for any reason."
- "A user must not write down their network access details (including passwords) anywhere nor let any computer they are using save/remember their password."
- "Users must not divulge their personal network access details, including passwords or other network access tokens, to anyone else, including managers or systems administrators."
- "All user account passwords must be a minimum of 8 characters long, include both alpha and numeric characters and must not contain a User's "User Account Name" be anything to do with the User's real name."
- "Users must either log off from the computer network and / or shutdown their computer when leaving the office for the day."
- "Computers must be configured to go into a locked state after 10 minutes of inactivity. The Users using the Application Software in a Client Server environment, will find "Session Timeout" in case of client's inactivity."

****

Appendix C

Internet Usage Policy

- "Users must not post on public discussion groups, chat rooms, or other public forums on the Internet unless the material is approved by the Nodal Officer of the Bank or any other authorized official of the Bank "
- "Nodal Officer / authorized official of the Bank may order the removal of any Internet posting by any the User that is deemed inappropriate or potentially damaging to the Bank's reputation."
- "Users must not download free software (executable files) from the Internet except with the prior approval of the Computer Cell officials".
- "Users may download data files from the Internet, but must check these files for viruses before using them (decompression and decryption, when they are used, must be performed first)".
- "Users must not send any sensitive information such as credit card numbers, telephone calling card numbers, fixed passwords, or customer account numbers through the Internet unless the connection or data is encrypted."
- "Users must not include SENSITIVE information in electronic mail messages sent through the Internet unless these messages are encrypted with an authorised encryption mechanism."
- "The establishment of any network connection with a third party (such as an "extranet") is forbidden unless the Nodal Officer of the Bank has given prior approval to the controls associated with this connection."
- "Users must not establish any web pages or other mechanism that provides public access to information about the Bank."
- "Users must not misrepresent, spoof, obscure, suppress or replace their own or another User's identity on the Internet."

****

Appendix D

Policy relating to External Storage

- "All Pen/Zip/Flash Drives are to be acquired through the General Branch of the Bank.

- "Subject to approval of the Branch In-charge and depending upon requirement, an employee will be assigned only one Pen/Zip/Flash Drives drive at a time. Additional Pen/Zip/Flash Drive can be acquired, in exceptional cases."

- "The Pen/Zip/Flash Drive shall be the property of the Bank and will be returned whenever the employee retires/ transferred or is asked to by the Nodal Officer."

- "The Pen/Zip/Flash Drive shall be produced for inspection by the Nodal Officer, whenever required."

- "The Pen/Zip/Flash Drive will be used for storing official data only. Personal data will not be allowed to be stored."

- "Un-authorised software is not to be installed by the user from or on the Pen/Zip/Flash Drive. Computer Cell officials shall install any software, if required by the user."

- "Prior to using the Pen/Zip/Flash Drive on the Desktop Computer, every user is required to scan the same or get it scanned from Computer Cell officials, for virus, malware, adware etc. and clean it. The user shall be fully responsible for any virus transmitted through the Pen/Zip/Flash Drive and shall have to face the consequences."

- "Every owner of Pen/Zip/Flash Drive provided by the Bank is required to properly maintain the equipment. The Pen/Zip/Flash Drive should be properly plugged in & out of the computer system."

- "The confidentiality / security of the Bank's data should not be compromised by the user by taking the confidential data out of the Bank's premises and misusing it."

- "Lost/damaged pen drives are required to be immediately reported to General Branch."

****