IT Policy - Operational Guidelines

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: -

Guidelines guide through a process or a task. They give general recommendations of how to perform a task, or advice on how to proceed in a situation. They usually provide a good overview of how to act in a situation where there's no specific policy or standard.

This document provides guidelines for issues like purchase, compliance, IT support and grievance redressal of the employees pertaining to IT Resources and services used for office work. These guidelines will serve as an institutionalized framework for management of IT resources and information.

2. Objective of the Operational Guidelines: -

The primary motive of the guidelines is to lay down standards and recommendations for legal and ethical management of information and IT resources of the Bank and to ensure safe practices. It would also define the principles to identify the people responsible for its enforcement and aims to define clear delegation of authority and responsibilities.

3. Scope of the Operational Guidelines: -

These guidelines apply to all the IT resources of the Bank and all the data and information created, generated, collected, and processed by the Bank.

4. Guidelines regarding Use of Disclaimers –

- Any private use of external communications such as e-mail / social media post, or any external communication that represents a personal view, must be clearly identified as such by way of a disclaimer.
- The disclaimer should automatically appear on the bottom of all outgoing emails / posts.

5. Guidelines regarding Information Disposal –

While disposing of hardware or media, a user must ensure that no information is disposed of unless its disposal is permitted by the **Right to Information Act 2005.**

6. Guidelines regarding Access to Information –

- Access rights should only be granted for the period that the user holds the role.
- As a user move into different role, his/her user profile must be changed accordingly to reflect the access rights of his/her new role.
- When a user no longer performs a role for the Bank, all of his/her user rights must be removed.

7. Guidelines regarding Remote Access of Bank's Network–

Remote access of Bank's network is permissible only if it is possible to -

- authenticate and allow access for third party support
- authenticate and allow access for legitimate users and deny all other access.

8. Guidelines regarding Third Party Access –

Vendors will request remote access during technical upgrade of their product or as part of installation process. The I.T. Official who is assigned to work with the vendor will assess / evaluate the vendor's requirements and subsequently, provide the required information/access.

9. Recommended measures to prevent/avoid VIRUS problems: -

- Always run the corporate standard, supported anti-virus. Download and run the current version; download and install anti-virus software updates as they become available.
- NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then delete them by emptying the Recycle Bin, as well.
- Delete spam, chain, and other junk email without forwarding, in with SADB's *Acceptable Use Policy*.
- Never download files from unknown or suspicious sources.
- Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
- Always scan a USB drive/ diskette from an unknown source for viruses before using it.
- Back-up critical data and system configurations on a regular basis and store the data in a safe place.
- New viruses are discovered almost every day. Periodically check the *Anti-Virus Policy* and the Recommended Processes list for updates.
- All machines that are infected with spyware must be cleansed with approved antivirus and antispyware software.

- All machines that are compromised must have their disks reformatted and the operating system and other programs reinstalled from scratch. When the machine is rebuilt, it must not be connected to a computer network until all software patches have been applied.

10. Guidelines regarding handling Hardware –

- While travelling, users should carry Laptop as hand luggage wherever possible.
- Portable devices add another dimension to the problem of information security. Always protect a portable device like Floppy, Pen Drive, External Hard Disk, External SSD etc. with a password and configure the device to shut down (or lock in some other way) after a period of inactivity.
- If the Bank's equipment (e.g. Desktop, Laptop, UPS etc.) is lost or stolen, the officials of Computer Cell of the Bank must be informed immediately and a note/report forwarded as soon as possible detailing the circumstances of the loss and information stored on the device.
- Ensure to keep your computer system e.g. desktop printer ups etc. neat and clean.

11. Guidelines regarding Passwords –

Recommendations for setting up passwords: -

- Must contain both upper-case and lower-case characters (e.g., a-z, A-Z)
- Must have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Must have at least eight alphanumeric characters long
- Should not have a word in any language, slang, dialect, jargon, etc.
- Should not be based on personal information, names of family, etc.
- Try to create passwords that can be easily remembered.

Password "Don'ts":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't reveal a password to co-workers while on vacation.
- Passwords should never be written down or stored on-line.

12. General Guidelines: -

- Branch Heads must ensure that all Users employed or working in, or engaged by, their department, are also aware of, are provided with or have access to, and comply with the Acceptable Use Guidelines and other security policies.

- All security measures must conform to the established Bank policies and applicable Government regulations/directions and those outlined in this document. The policies in this document are consistent with, but independent of, other Bank policies.

****