IT4

Category: Information Technology

WORKSTATION SECURITY POLICY

I. PURPOSE

The purpose of this policy is to ensure the security of Pioneer Community Energy's (Pioneer) Information Systems, workstations, and data.

II. SCOPE

This policy applies to all Pioneer employees and affiliates.

III. POLICY

This Policy helps ensure that access to sensitive information is restricted to authorized users. By following appropriate security measures, Staff can help ensure information integrity, confidentiality, and availability.

Staff shall follow appropriate guidelines and procedures when using workstations and systems. Pioneer has implemented certain technical, physical, and administrative controls and safeguards to ensure that workstations restrict access to authorized users.

Physical access to workstations shall be restricted to only authorized personnel. Staff shall prevent unauthorized viewing of information on a screen:

- Staff shall ensure that monitors are positioned away from public view. If necessary, install privacy screen filters or other physical barriers to prevent public viewing.
- Staff shall manually activate a password protected screen saver when they leave their desk.
- Systems shall have a password protected screen saver activated within a short timeout period to ensure that workstations that were left unsecured are protected.

Prior to leaving for the day, staff shall:

- Exit running applications and close any open documents.
- Ensure workstations are left on as recommended by IT staff but logged off in order to facilitate after hours updates.

Adopted: October 21, 2021
Resolution 2021-38

Staff shall comply with all applicable IT policies and procedures when accessing information resources.

Staff shall use workstations for authorized business purposes only.

Staff shall only use Pioneer issued mass storage devices such as USB drives. These devices should be treated as sensitive information and be secured in a locked drawer.

All sensitive information must be stored securely. Sensitive information shall be encrypted and comply with Pioneer's Encryption Policy. Laptops containing sensitive information shall have the hard drives encrypted.

The IT Department should ensure that all workstations use a surge protector (not just a power strip) or a UPS battery backup. Pioneer recommends staff keep food and drink away from workstations to avoid accidental spills.

Workstations shall have vendor-issued critical security updates and patches installed in a timely manner.

Workstations shall have active and updated anti-malware protection software. Staff shall not disable anti-malware protection software. See Anti-Malware Policy for more information.

Each workstation shall have an active software firewall that protects the device from external threats. Staff shall not disable the firewall.

IV. DISTRIBUTION

This policy is to be distributed to all Pioneer staff who use Information Resources.