



Policy IT006: Information Security Policy

Recommended for Approval by: Fawn J. Petrosky
Fawn Petrosky, Vice President for Finance

Approved by: Dr. Dale-Elizabeth Pehrsson
Dr. Dale-Elizabeth Pehrsson, President

Effective Date: 2/24/2023

A. Intent

This policy describes the requirements for securing computing and network connected devices and protecting confidential Pennsylvania Western University (PennWest) data. It includes a baseline set of requirements for all computing devices that connect to PennWest's Network. The policy also provides best practice recommendations to guide users, administrators, and University Technology Services staff in further steps to protect PennWest's computing and network infrastructure and data.

Computer and data security is each person's responsibility. Every computer user is responsible for securing and protecting the information technology resources and data over which he or she has control by following the guidance presented in this document. In addition to this document, you are to comply with all PennWest security policies and procedures.

The purpose of the policy is to protect the confidentiality, integrity, availability, and accountability of University data, and to protect PennWest's computing and network infrastructure.

B. Definition(s)

- **Availability** - Ensuring timely and reliable access to and use of information.
- **Confidentiality** - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- **FTP –File Transfer Protocol** – is a standard network protocol used to transfer files from one host to another.

- **HTTP -Hypertext Transfer Protocol Service** – Having this service turned on makes the system a Web Server.
- **Integrity** - Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.
- **Mobile Device** - A mobile device may be described as a handheld computer that does not run a full version of Windows, Mac OS X or Linux. Examples include: iPhone OS, Blackberry OS, and Android OS.
- **Multi-Factor Authentication (MFA)** - An authentication system that requires more than one distinct authentication factor for successful authentication.
- **OS – Operating System** – Is a collection of software that manages hardware resources and provides common services for programs.
- **SNMP- Simple Network Management Protocol** – is a protocol for managing devices on IP networks.
- **telnet** – is a network protocol used to provide text-based, unencrypted communication.

C. Policy

Basic Requirements for Computers/Laptops connecting to PennWest Network:

- **Passwords**
 - Devices must be protected by strong passwords that are resistant to dictionary attacks.
 - Default passwords and blank passwords must never be used.
 - Passwords must be encrypted in transit and in storage.
 - Guest or anonymous access must be disabled.
 - The use of group, shared, or generic accounts and passwords is prohibited.
- **Additional Security Requirements**
 - Devices must run a supported operating system (OS).
 - Unneeded Services- Disable or uninstall any unneeded services. If you do not use services such as ftp, telnet, snmp, http, etc. then they should be disabled.
 - Use Secure Protocols- Use protocols such as ssh instead of telnet, sftp instead of ftp, https instead of http, and SNMPv3 instead of SNMP. Telnet, ftp, http, and SNMP are unencrypted (clear-text) protocols.
 - Security Patches – Security patches shall be applied within one month of release.

- Network devices and supported Internet of Things (IoT) devices must have their firmware and software regularly updated. The support of these devices on the network is up to IT discretion.
- Antivirus Software – Devices running Windows and Macintosh Operating Systems must run antivirus software with automatic definition and program updates.
- Computer programs and applications (e-mail clients, browsers, productivity programs, etc) must be kept up to date.
- Endpoint devices that support firewalls are required to run their firewall software.
- **Mobile Device Security Requirements**
 - Enable password protection and require complex passwords.
 - Install only applications that you need.
 - Updating – Mobile device operating systems and applications must be updated regularly. Select the automatic update option if available.
 - You must not store sensitive or confidential information on mobile devices.
 - Limit Risk of Theft – Avoid leaving the device in public places, visible in a parked car, or checked with luggage during flight. Never leave your device unattended.
 - Delete all information stored in a device prior to discarding, exchanging, or donating it.
 - All wireless communication (i.e. Bluetooth, wifi, etc.) should be turned off when not in use.
- **Physical Security**
 - Physically secure any resource that you manage or own.
 - Keep areas with computer and network equipment locked when unattended.
 - Do not leave portable devices, USB drives, cell phones, or other media in open areas.
 - Printers that print sensitive documents should be kept in areas with restricted access.
 - Lock your Desktop when you are away from your computer.
 - Do not write passwords down and post them at your work area.

Roles and Responsibilities

The following section describes the individuals and/or areas involved in the development,

maintenance and execution of PennWest's Information Security Policy and their role and responsibilities.

- **Information Security Leadership** -is responsible for determining methods of implementing and enforcing security policies and for advising the enterprise on security-related issues. The leader ensures that information security awareness is increased, and audits are performed and reported regularly. The leader appoints and manages suitably skilled people to staff information security teams as deemed appropriate, and the leader has the authority to request the appointment of security representatives in business units.
- **Human Resources / Payroll** - Responsible for providing appropriate information security orientation for new employees and retention of employee acknowledgement of Information Security Program Compliance.
- **Cabinet** - is accountable for compliance, risk, and security and must ensure compliance with policies, standards, procedures and practices within their respective areas of responsibility.
- **All Users including faculty, staff, students, contractors, and guest users of PennWest** - Every computer user is responsible for securing and protecting the information technology resources and data over which he or she has control. In addition, you are to comply with all PennWest Policies and Procedures.
- **Third Parties/Vendors** - It is expected that strategic systems not under the direct control of PennWest, such as those operated or maintained by vendors, will adhere to similar standards as PennWest.
 - Remote Access Accounts for vendors are to be disabled when not in use.
 - Remote Access Technologies for Third Party/Vendor use is only to be activated when needed and is to be deactivated immediately after use.
 - Remote access will use Multi-Factor Authentication (MFA).

Noncompliance

- Any University assets or personally owned technologies that are deemed not in compliance with this policy may be disconnected from the network without notice at the discretion of University Technology Services.

D. Procedure(s)

Not applicable.

E. Related policies

Acceptable Use Policy.

F. Contact Information

Information Technology Services

G. Policy Review Schedule

All policies will be reviewed every two years or on an as needed basis if a change in BOG, PASSHE or

Pennsylvania law would create the need for an immediate change.