Policy IT010: Information Technology Incident Reporting and Response Policy

Recommended for Approval by: Fawn L. Petrosky

Fawn Petrosky, Vice President for Finance

Approved by: Dale-Elizabeth Pehrsson

Dr. Dale-Elizabeth Pehrsson, President

Effective Date: 2/24/2023

A. Intent

This policy serves to minimize the negative consequences of an Information Security incident (as defined below) and to improve the Pennsylvania Western University's (PennWest) ability to promptly restore operations affected by such incidents. The University's goal is to assure that incidents are promptly reported to the appropriate University officials, that they are consistently and expertly responded to, and that serious incidents are properly monitored.

The purpose of information security incident response is:

- To ensure that incidents are promptly reported to the appropriate University officials.
- To mitigate the effects caused by such an incident.
- To protect the information resources of the University from future unauthorized access, use or damage
- Ensure that PennWest fulfills all of its obligations under University policy, and federal and state laws and regulations with respect to such incident

B. Definition(s)

- **Information Technology Asset** - A system or systems comprised of computer hardware, software, networking equipment, and any data on these systems. Such assets include but are not necessarily limited to desktop computers, servers, printers, telephones, network equipment, E-mail and web based services.

- **Security Incident** – an incident meeting one or more Security Incident of the following conditions:
  - o A breach, attempted breach or other Unauthorized Access of a PennWest Information

Technology Asset. The incident may originate from the PennWest network or an outside entity.

o Any Internet worms or viruses.

o Disruption of information technology service levels.

o Theft or loss of a laptop, desktop, PDA or other electronic device that may contain confidential or sensitive data.

o Web site defacement.

o Compromised password(s).

o Unauthorized use of an individual's computing account.

o Any activity that harms or represents a serious threat to the whole or part of PennWest's computer, telephone and network-based resources.

C. Policy

• **Who should report a security incident?** Any person (Faculty, staff, and student) who knows or reasonably believes that a Security Incident involving a PennWest-owned Technology Asset has occurred. If it is unclear as to whether a situation should be considered a Security Incident, it should be reported so that Information Technology Services can evaluate the situation.

• **How do you report a security incident?** Security incidents must be reported as soon as possible by calling our Helpdesk at the numbers below during normal business hours. Go to the Information Technology Services website https://itservices.pennwest.edu/ for off hours reporting instructions.

724-938-5911 California Campus
814-393-2640 Clarion Campus
814-732-2111 Edinboro Campus

Anyone who discovers a weakness or vulnerability in the information security measures used by PennWest must not discuss these matters with anyone other than the IT Security Team.

• **Response** – Once reported, the Information Security Team will investigate, assess, and respond to threats to PennWest IT resources.

Incidents may be reported to the appropriate law enforcement, PASSHE, or University officials where the circumstance dictates. The IT Security Team will handle these notifications.

Any University information technology assets or personally owned technologies that pose a security threat may be disconnected from the network. If a security breach is discovered in progress, the Incident Response Team may take immediate actions to isolate and deny access to the user, data or information technology asset.

D. Procedure(s)

Not applicable.

E. Related policies

Not applicable.

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.