Policy IT025: Information Technology Security Program Policy

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

Approved by: Dr. Dale-Elizabeth Pehrsson, President

Effective Date: 2/24/2023

A. Intent

The intent of this policy is to define the framework that will be used to protect data and other information security assets at Pennsylvania Western University (PennWest). Unfortunately, there is no single defense mechanism that can be deployed to protect a technology environment. A Defense in Depth approach that layers a series of defense mechanisms such that if one fails, another will already be in place to thwart the attack will be used.

PennWest has a complex and resource rich information technology environment upon which there is increasing reliance to provide mission-critical academic, instructional, and administrative functions. Safeguarding the Institution's technology assets in the face of growing security threats is a significant challenge requiring a strong, persistent, and coordinated program that leverages widely accepted, effective security practices appropriate for the higher education environment. This policy states the codes of practice with which the University aligns its Information Technology Security Program. The primary goal of the Information Technology Security Program is to protect the confidentiality, integrity, and availability of University information assets, to protect against anticipated threats or hazards to the security and integrity of information, and to protect against unauthorized access to information that could result in substantial harm to any student, faculty, or staff.

B. Definition(s)

- **Defense in Depth** – is the concept of protecting a computer network with a series of defensive mechanisms such that if one mechanism fails, another will already be in place to thwart an attack.
- **Family Educational Rights and Privacy Act (FERPA)** - is a United States federal law. FERPA gives parents access to their child's education records, an opportunity to seek to have the records amended, and some control over the disclosure of information from the records.

- **General Data Protection Regulation (GDPR)** - is a regulation in EU law on data protection and privacy for all individuals within the European Union. It addresses the export of personal data outside the EU.
- **Gramm-Leach-Bliley Act (GLBA)** - also known as the Financial Modernization Act of 1999, is a federal law enacted in the United States to control the ways that financial institutions deal with the private information of individuals.
- **Health Insurance Portability and Accountability Act (HIPAA)** - a US law designed to provide privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals, and other health care providers. Developed by the Department of Health and Human Services, these new standards provide patients with access to their medical records and more control over how their personal health information is used and disclosed.
- **Payment Card Industry Data Security Standard (PCI DSS) Compliance** - is adherence to the set of policies and procedures developed to protect credit, debit and cash card transactions and prevent the misuse of cardholders' personal information. PCI DSS compliance is required by all card brands.
- **Red Flags Rule** - was created by the Federal Trade Commission (FTC), along with other government agencies such as the National Credit Union Administration (NCUA), to help prevent identity theft.

C. Policy

The University's Information Technology Security Program will be based upon best practices recommended in "CIS Controls" published by the Center for Internet Security, and "Code of Practice for Information Security Management" published by the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC 27002), appropriately tailored to the specific circumstances of the University. The program will also incorporate security requirements of applicable regulations, such as the Family Educational Rights and Privacy Act (FERPA), Gramm-Leach-Bliley Act (GLBA), Payment Card Industry (PCI) Data Security Standard, Red Flags Rule, General Data Protection Regulation (GDPR), and the Health Insurance Portability and Accountability Act (HIPAA). Professional organizations, such as EDUCAUSE and the National Institute of Standards and Technology (specifically NIST Special Publication 800-171) will serve as resources for additional effective security practices. The University Information Technology group will continue to update and follow best practices of any new data laws not mentioned herein that become law between policy revisions.

References

- "Code of Practice for Information Security Management" (ISO/IEC 27002). This international standard defines guidelines and general principles for the effective management of information security within an organization. It is a risk-based framework widely used to guide establishment of security standards and management practices. http://www.iso27001security.com/html/27002.html
- EDUCAUSE is a nonprofit association dedicated to the advancement of higher education through the effective use of information technology. Members include representatives from institutions of higher education, higher education technology companies, and other related organizations. http://www.educause.edu
- International Organization for Standards (ISO). The world's largest developer of standards, the organization is made up of representatives from governmental and private sector

standard bodies, e.g. the American National Standards Institute. http://www.iso.org/iso/home.html

- International Electrotechnical Commission (IEC). The IEC is a global organization that develops and publishes standards addressing electrical, electronic, and related technologies. Membership comes from government, the private sector, consumer groups, professional associations, and others. http://www.iec.ch/
- Center for Internet Security (CIS). The Center for Internet Security (CIS) is an organization dedicated to enhancing the cybersecurity readiness and response among public and private sector entities. CIS is home to the Multi-State Information Sharing and Analysis Center (MS-ISAC), CIS Security Benchmarks, and CIS Critical Security Controls. https://learn.cisecurity.org/20-controls-download
- National Institute of Science and Technology (NIST). NIST promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security. https://www.nist.gov/

D. Procedure(s)

Information Technology Services will conduct an annual assessment of the cyber-security posture of the University in partnership with University leadership and PASSHE.

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.