Policy

Title:	Cyber-Security Training
Effective Date:	March 30, 2022
Approved By:	President's Council
Responsible Party:	Vice President of Technology and Learning Resource Services
History:	N/A
Related Documents: Use of Electronic Communications	

I. PURPOSE

The purpose of this policy is to ensure that security awareness and training controls protect Salus University's information systems, Protected Health Information (PHI) and Personally Identifiable Information (PII) to ensure information availability, confidentiality, and integrity of data.

II. DEFINITION

N/A

III. POLICY

All Faculty and Staff employed by Salus University will be required to undergo Cybersecurity Awareness Training on a regular basis. This is to ensure that all faculty and staff members are aware of their role in keeping the Salus University's data assets confidential, available, and secure.

IV. PROCEDURE

A. General

The Associate Director of Network and Security Services shall be responsible for developing, implementing, and maintaining a Security Awareness and Training Plan. This plan will document the process for Faculty and Staff security training, education, and awareness and ensure that all Salus University employees understand their role in protecting the confidentiality, integrity, and availability of data assets. The plan will cover what information to communicate, when to communicate it, with whom to communicate,

responsibility for communication, and the process by which communication shall be implemented.

The plan shall ensure that Faculty and Staff are provided with regular training, reference materials, supports, and reminders that enable them to appropriately protect Salus University data assets. Training will include, but is not limited to:

- Responsibilities for protecting sensitive information
- Risks to information assets and resources
- Data encryption and access management
- Secure use of data and information assets
- Salus University information security policies, procedures, and best practices
- Protecting assets and identities

B. Training Plan Requirements The

training plan shall ensure:

- All Salus University employees attend an approved security awareness training class within thirty (30) working days of being granted access to Salus University resources.
- Training may be in the form of recorded videos, printed materials, external links and potentially purchased external training.
- Faculty and Staff may receive training appropriate for specific job roles and responsibilities. After such training, the employee must verify through certificate completion and assessment that they received the training, understood the material presented, and agrees to comply with it.
- Faculty and Staff are trained on how to identify, report, and prevent security incidents and data breaches.
- Appropriate security policies, procedures, and manuals are readily available for reference and review.
- Staff annually attend or view security awareness refresher training.

- Employees sign an acknowledgement stating they have read and understand Salus University acceptable use requirements regarding computer and information security policies and procedures.

- Faculty and Staff are provided with sufficient training and supporting reference materials to allow them to protect Salus University data and assets.

- Cloud computing and outsourcing security awareness training shall address a pre-defined scope of deliverables.

- Staff are aware and accept the risks, responsibilities, and limitations related to the Acceptable usage policy.

C. Implementation

The Associate Director of Network and Security Services or their designee shall:

- Develop and maintain a communications process to communicate new security programs and items of interest.

- Ensure that Faculty and Staff that are responsible for implementing safeguards receive training in security best practices.

- Ensure periodic security reminders (flyers or posters, emails, verbal updates at meetings) keep Salus University staff up-to-date on new and emerging threats and security best practices. The frequency and method of delivery of such reminders shall be determined by the Associate Director of Network and Security Services

D. Audit Controls and Management

On-demand documented procedures and evidence of practice shall be in place for this operational policy as part of Salus University internal operations. Examples of management controls include:

- Documented information security training plan with evidence of consistent update and version control of the document
- On-demand review of existing training program information and implementation within the organization
- On-demand evidence of continuing education and reminders are in place