FERRIS STATE UNIVERSITY

DIVISION OF ADMINISTRATION AND FINANCE

Security Awareness Training & Testing

Administration and Finance Business Policy

Policy Number: 2025:XX
New Policy

This Policy establishes the requirements for all University employees to assist in protecting the University's information assets by completing, at least annually, security awareness training and testing.

SCOPE AND APPLICABILITY

This policy applies to all members of the FSU community and applies to all locations and operations of FSU including, but not limited to, University employees, affiliates, student employees, students, alumni, vendors, emeriti, retirees, guests, and contractors.

The purpose of this Security Awareness and Training Policy is to educate our users of their responsibility to help protect the confidentiality, availability, and integrity of Ferris State University's information assets and to ensure that all users are trained on relevant rules, regulations, and best practices for information security.

DEFINITIONS

Phishing
Emails that masquerade as a reputable entity to lure individuals into revealing sensitive data.

Vishing
Phone calls or voice messages that masquerade as a reputable entity to lure individuals into revealing sensitive data.

Smishing
Text messages that masquerade as a reputable entity to lure individuals into revealing sensitive data.
Social Engineering
A technique used to manipulate people into performing actions or sharing sensitive information.
Malware
Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

USB Testing
The practice of testing how users react upon finding an unknown USB drive.

Physical Security Assessments
The process of identifying and analyzing physical threats and vulnerabilities to the organization's information security and evaluating and improving security measures to mitigate or remediate these risks.

Health Insurance Portability and Accountability Act (HIPAA)
The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that requires the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge.

Family Rights and Privacy Act (FERPA)
The Family Educational Rights and Privacy Act (FERPA) is a federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

Payment Card Industry (PCI) Data Security Standard
An information security standard administered by the Payment Card Industry Security Standards Council for organizations that handle branded credit cards from the major card schemes.

POLICY

The Information Security Office will implement, maintain, and provide an ongoing university-wide information security awareness program that will use various training techniques, including email, university-wide communications, webpages, and security awareness platform(s) deemed appropriate by the Information Security Manager. The program will consist of training and testing.

The Information Security Manager is responsible for the oversight of the program, including development, implementation, and testing. Training for all employees is automatically tracked and monitored to ensure compliance.

Training

All university employees are required to complete annual information security awareness training to help understand their responsibility in safeguarding systems and data. Automatic emails will be sent to employees when training campaigns begin, reminders to complete training, past due reminders, and/or upon completion of training.

Training may include various security topics such as, but not limited to:

- Phishing
- Social engineering
- Red flags
- Social media
- Mobile devices
- Malware
- Passwords
- HIPAA
- FERPA
- PCI

New Hire Security Awareness Training

Newly hired employees must complete an initial information security awareness training campaign within 30 days of hire. New hires are automatically enrolled in the initial training campaign.

Annual Security Awareness Training

Employees must complete annual security awareness training within each fiscal year. Supervisors are encouraged to ensure each employee under their supervision has completed the security awareness training.

Remedial Training

If employees fail to complete training or testing exercises, they may be required to complete remedial training courses or may be required to participate in remedial training exercises with members of the Information Security department as part of a risk-based assessment.

Additional Training for Specific Roles

Certain staff may be required to complete additional training modules depending on their job requirements upon hire and at least annually.

Additional Training

Training beyond the university-required training can be requested by employees or supervisors at any time and will be delivered if available. Please contact the Information Security office for additional information on what additional training is available or to discuss your specific needs.

Testing

The FSU Information Security department will conduct periodic simulated social engineering exercises including but not limited to phishing (e-mail), vishing (voice), smishing (SMS), USB testing, and physical security assessments. Information Security will conduct these tests randomly throughout the year and may conduct targeted exercises against specific departments or individuals based on a risk determination.

CORRESPONDING POLICIES

Information Security Policy

CONTACTS

For more information, please contact the following departments:
Finance Office and/or Chief Information Officer

Amanda Matheson
Vice President for Administration & Finance