ENTERPRISE IT STANDARDS AND PROCEDURES: SECURITY AWARENESS TRAINING AND TESTING

Policy: Information Technology Security
Document: Security Awareness Training and Testing Standards & Procedures
Campus: MSU-Northern
Revised Date: April 2023
Review Date: April 2025
Contact: Chief Information Officer

Technical security controls are a vital part of our information security framework but are not in themselves sufficient to secure all information assets. Effective information security also requires the awareness and proactive support of all employees, supplementing and making full use of the technical security controls. This is obvious in the case of social engineering attacks and other current exploits being used, which specifically target vulnerable humans rather than IT and network systems.

Lacking adequate information security awareness, employees are less likely to recognize or react appropriately to information security threats and incidents, and are more likely to place information assets at risk of compromise. In order to protect information assets, all workers must be informed about relevant, current information security matters, and motivated to fulfill their information security obligations.

Scope

This policy applies to all organizational units within MSU-Northern. It applies regardless of whether employees use computer systems and networks, since all employees are expected to protect all forms of information assets including computer data, written materials/paperwork, and intangible forms of knowledge and experience.

Awareness training must fulfill the requirements for the security awareness program as listed below:

- The information security awareness program should ensure that all employees achieve and maintain at least a basic level of understanding of information security matters, such as general obligations under various information security policies, standards, procedures, guidelines, laws, regulations, contractual terms, and generally held standards of ethics and acceptable behavior.
- Additional training is appropriate for employees with specific obligations towards information security that are not satisfied by basic security awareness, for example Information Risk and Security Management, Payment Card Industry Data Security Standard (PCI-DSS), Security Administration, Site Security and IT/Network Operations personnel. Such training requirements must be identified in departmental/personal training plans and funded accordingly. The training requirements will reflect relevant prior experience, training and/or professional qualifications, as well as anticipated job requirements.
- Security awareness and training activities should commence as soon as practicable after employees join the organization. The awareness activities should continue on a continuous/rolling basis thereafter in order to maintain a reasonably consistent level of awareness.
- Where necessary and practicable, security awareness and training materials and exercises should suit their intended audiences in terms of styles, formats, complexity, technical content, etc. Everyone needs to know why information security is so important, but the motivators

may be different for workers focused on their own personal situations or managers with broader responsibilities to the organization and their staff.
- The University will provide employees with information on the location of the security awareness training materials, along with security policies, standards, and guidance on variety of information security matters.

Information Security Awareness Training

MSU-Northern requires that each employee upon hire and at least once per academic year thereafter successfully complete Security Awareness Training assigned to them and to be completed online. Certain employees may be required to complete additional training modules depending on their specific job requirements upon hire and at least once per academic year. Employees will be given a reasonable amount time to complete each course so as to not disrupt business operations.

Simulated Social Engineering Exercises

MSU-Northern will conduct periodic simulated phishing (e-mail) exercises, and may conduct other periodic simulated social engineering including but not limited to vishing (voice), smishing (SMS), USB testing, and physical assessments. MSU-Northern will conduct these tests at random throughout the year with no set schedule or frequency. Testing may involve targeted exercises against specific departments or individuals based on a risk determination (see Appendix B).

Compliance & Non-Compliance

Compliance with this policy is mandatory for all employees, including executives. The MSU-Northern ITS department will monitor compliance and non-compliance with this policy and report to the executive team the results of training and social engineering exercises.

The penalties for non-compliance are described in Appendix A of this policy.

Non-Compliance Actions

Certain actions or non-actions by MSU-Northern personnel may result in a non-compliance event (Failure).

Failure to complete assigned training by the end of the training period may result in email access being revoked.

Other Failures include but are not limited to:

- Failure to complete required additional assigned training within the time allotted
- Failure of a social engineering exercise
- Clicking or responding in some manner to an actual phishing email

Failure of a social engineering exercise includes but is not limited to:

- Clicking on a URL within a phishing test
- Replying with any information to a phishing test
- Opening an attachment that is part of a phishing test
- Enabling macros that are within an attachment as part of a phishing test
- Allowing exploit code to run as part of a phishing test
- Entering any data within a landing page as part of a phishing test
- Transmitting any information as part of a vishing test
- Replying with any information to a smishing test
- Plugging in a USB flash drive as part of a social engineering exercise
- Failing to follow company policies in the course of a physical social engineering exercise

Certain social engineering exercises can result in multiple Failures being counted in a single test. The maximum number of Failure events per social engineering exercise is two.

The MSU-Northern ITS department may also determine, on a case by case basis, that specific Failures are a false positive and should be removed from that employee member's total Failure count.

3.2 Compliance Actions

Certain actions or non-actions by MSU-Northern personnel may result in a compliance event (Pass).

A Pass includes but is not limited to:

- Successfully identifying a simulated social engineering exercises
- Not having a Failure during a social engineering exercise (Non-action)
- Reporting real social engineering attacks to the ITS Help Desk

Removing Failure Events through Passes

Each Failure will result in a remedial training or coaching event as described in Appendix A of this document. Subsequent Failures will result in escalation of training or coaching. De-escalation will occur when three consecutive Passes have taken place.

Responsibilities and Accountabilities

Listed below is an overview of the responsibilities and accountabilities for managing and complying with this policy program.

The Chief Information Officer is accountable for running an effective information security awareness and training program that informs and motivates workers to help protect the organization's and the organization's customer's information assets.

The Chief Information Officer is responsible for developing and maintaining a comprehensive suite of information security policies (including this one), standards, procedures and guidelines that are to be mandated and/or endorsed by management where applicable. Working in conjunction with other university functions, it is also responsible for conducting suitable awareness, training, and educational activities to raise awareness and aid understanding of employee's responsibilities identified in applicable policies, standards, and laws.

All Managers are responsible for ensuring that their staff and other workers within their responsibility participate in the information security awareness, training, and educational activities where appropriate and required.

All employees are personally accountable for completing the security awareness training activities, and complying with applicable policies, laws, and regulations at all times.

MSU-Northern reserves the right to update or revise these standards or implement additional policies and procedures in the future. Users are responsible for staying informed about and compliance with university policies and procedures regarding the use of computing and communication technology.

Appendix A – Schedule of Failure Penalties

The following table outlines the penalty of non-compliance with this policy. Steps not listed here may be taken by the MSU-Northern Information Technology Services team to reduce the risk that an individual may pose to the company.

Failure Count	**Resulting Level of Remediation Action**
First Failure	Mandatory completion of an additional online security training module.
Second Failure	Mandatory completion of additional online security training modules.
Third Failure	Mandatory completion of additional online security training modules.
Fourth Failure	Face to face meeting with their manager
Fifth Failure	Face to face meeting with their manager and Head of Human Resources
Sixth Failure	Face to face meeting with the CIO and the Head of Human Resources - Possibility that additional administrative and technical controls will be implemented to prevent further Failure events
Seventh Failure	Meeting with CIO, Chancellor or Provost, and Head of Human Resources - Possibility that additional administrative and technical controls will be implemented to prevent further Failure events
Eighth Failure	Formal review of employment with Head of Human Resources - Possibility that additional administrative and technical controls will be implemented to prevent further Failure events
Ninth and Subsequent Failures	Potential for Termination of Employment or Employment Contract

Appendix B – Methods for Determining Employee Risk Ratings

The following is a list of situations that may increase a risk rating of an MSU-Northern employee. Higher risk ratings may result in an increased sophistication of social engineering tests and an increase in frequency and/or type of training and testing.

- Employee email resides within a recent Email Exposure Check report
- Employee is an executive or VP (High value target)
- Employee possesses access to significant company confidential information
- Employee possesses access to significant company systems
- Employee maintains a weak password
- Employee has repeated company policy violations