WAYNE STATE UNIVERSITY
Computing & Information Technology

Security Awareness Training Standard

Purpose
This standard establishes the need for the University to provide security awareness training to university constituents so they can be aware of common information security threats and use that knowledge to protect themselves, protect university data, and promptly report security incidents via the correct channels.

Scope
The scope of this standard covers all users of university-managed IT systems, including students, staff, faculty, guests, and other regular users of IT services.

Roles and Responsibilities
University staff members will take advantage of provided training materials to educate themselves on common security risks and the techniques attackers use when attempting to compromise data. Staff members handling confidential data in enterprise systems must complete trackable, assigned training curriculum to ensure a baseline level of security awareness for all handled confidential data.

University management will support and encourage training and learning of their employees, as well as review completion records and take appropriate action to ensure their employees have the proper knowledge and education to keep university data secure.

The C&IT Information Security Office will develop and/or deploy relevant security awareness training materials with the assistance of University marketing and C&IT Marketing and Service Management, incorporating feedback into continual education efforts.

Awareness and Training Standards, Procedures, and Guidelines
Detailed procedures, standards, and guidelines will be authored and maintained by the C&IT Information Security Office outlining the specific security awareness and training materials to be developed and implemented, along with appropriate guidance. New or modified procedures, standards and guidelines will be communicated to all University IT staff once approved by the C&IT Risk & Security Oversight Committee.

Organizational Coordination
The C&IT Information Security Office will solicit feedback from on-campus IT units regarding the effectiveness and applicability of this standard and related materials, taking it into consideration during

periodic standard reviews. This standard and associated documents will be openly published and communicated to all IT staff at a minimum of an annual basis.

Compliance
All university units are required to be in compliance with this and any associated standards. Any exceptions to this standard must be approved by the C&IT Information Security office, will be given a deadline for proper compliance, and will be reviewed on an annual basis.

Standard Review

This standard and any associated materials will be reviewed at a minimum on an annual basis by the C&IT Risk & Security Oversight Committee.

Definitions
As used in this standard, *"enterprise systems"* are electronic information systems maintained by C&IT that contain confidential institutional data. Current examples of enterprise systems include Banner, Cognos, and Imaging.

Standards for Security Awareness
The University must use and maintain the following controls to protect against and minimize the impact of security incidents:

1. New Employee Materials. As part of the employee onboarding process, basic security awareness training is provided by C&IT to all employees. Training content includes security basics, common threats, and how to recognize and report suspected security incidents.

2. Regular Training Updates. As part of ongoing education, security training updates are sent by C&IT to all employees on a monthly basis, as well as when significant information system changes occur. Updates consist of relevant security topics including information on insider threats, system updates, and how to recognize and report suspected security incidents.

3. Security Training Records. C&IT maintains records of security training and awareness activities, including sent and opened emails, as well as participation and completion of any in-person or online training sessions. Training records are preserved for a minimum of 12 months.

4. Role-Based Security Training. Employees with roles that include handling sensitive or confidential data are provided additional training materials relevant to their specific job roles and functions.

Additional Standards for Enterprise System Users

1. Required Training. Employees who access enterprise systems must successfully complete specific required online security awareness training modules as developed or deployed by C&IT. Completion of modules will be tied to the employee's AccessID and require complete viewing of content as well as passing applicable competency tests or exercises. Any required training must be completed before access to enterprise systems is given, and employees must retake the current versions of required training at a minimum every 24 months.

2. Reporting. Annual reports of security training activity will be provided to each Business Affairs Officer (BAO) regarding the activity and completion status for any employees in their division, as well as aggregate statistics for completion rates for each division at the University.