I. Overview
Protecting the confidentiality, integrity, and availability of U-M systems and data is the responsibility of all U-M employees. Accountability must be derived from a fully informed, well-trained, and aware workforce. By participating in information assurance awareness, training and education, members of the U-M community can help reduce the risk of data breaches, maintain compliance with applicable laws, regulations, and contractual agreements, and ultimately help protect U-M systems and data. This awareness has the additional benefit of providing individuals with the knowledge and skills that help them protect their own devices and data.

II. Scope
This Standard applies to the Ann Arbor, Dearborn, and Flint campuses, including all schools, colleges, institutes, and the U-M Health System. The scope includes awareness and training needs of all users of U-M information resources, and applies to all faculty, researchers, staff, workforce members, and students.

III. Definitions
Awareness: Security awareness efforts are designed to change behavior or reinforce good security practices. Awareness of policies, practices, and procedures are intended to allow individuals to recognize security concerns and respond accordingly to help maintain a secure environment for both institutional and personal information.

Training: Training strives to produce relevant and needed security skills and competency in faculty and staff who are not information assurance professionals. The content of training programs is designed to the requirements of specific target audiences.
Education: Education integrates all of the skills and competencies of the various functional specialties into a common body of specialized knowledge for staff with primary job responsibilities related to information assurance.

IV. Roles and Responsibilities

Chief Information Security Officer (CISO): The CISO is responsible for:

- Collaboratively establishing a university-wide awareness and training program strategy;
- Advocating that the university’s information assurance awareness and training program is adequately funded;
- Providing appropriate training and professional development opportunities for university staff with significant information assurance responsibilities;
- Collaborating with other institutional officials to ensure that the university has trained personnel sufficient to support institutional compliance with applicable laws and regulations.

Information and Infrastructure Assurance (IIA): IIA has day-to-day responsibility for information assurance awareness and related communications to the campus community. Specifically, IIA maintains the Safe Computing website and is responsible for issuing campus-wide awareness messages including alerts, advisories, and notices related to significant security threats or issues. In addition, IIA, in collaboration with other stakeholders:

- Promotes the professional development and certification of information assurance staff;
- Work to ensure that awareness and training materials are developed and disseminated to the intended audiences;
- Ensure that awareness and training material is reviewed periodically and updated when necessary.

Unit IT Managers and Security Unit Liaisons (SUL): Unit IT Managers and SULs should:

- Work with the CISO and IIA to meet shared awareness and training responsibilities; develop as appropriate and needed training and professional development opportunities for staff or users with significant security and information assurance responsibilities, including compliance with information security laws and regulations; and ensure that all users (including contractors) of their systems and applications are appropriately trained before allowing them access.

Users: Users are the single most important group of people that can help to reduce unintentional errors and IT vulnerabilities. Users include employees (faculty, researchers, clinicians, researchers, staff), affiliates, contractors and other third parties, alumni, and students. Users must: understand and comply with U-M information security policies, practices, and procedures; be sufficiently aware of their responsibility to follow the Proper Use of Information Resources (SPG 601.07); and be aware of actions they can take to better protect U-M information resources for which they are responsible as well as their own information.

V. Standard
The university is committed to design, develop, implement, and maintain an information assurance awareness and training program so that employees can best support the protection of its most sensitive institutional information assets.

U-M employees are expected to engage in periodic data protection awareness, training, and education campaigns. In addition, certain job functions or working with specific types of data may require additional specialized training or education.

Additional training opportunities include: attending technical seminars or online events; reading technical publications or books; attending a technical vendor product presentation; attending technical training for a vendor product; attending general IT training; completing a training program that leads to certification.

To ensure that U-M employees stay up-to-date on required training, it is recommended that participation in Information assurance training and awareness be included in staff performance evaluations.

The following table lists currently required role-based IT assurance training and education:

<p>| Employee Role                                                                 | Training                                                                 | Frequency                        | Department/Owner                        |
|------------------------------------------------------------------------------|--------------------------------------------------------------------------|--------------------------------cl|
| U-M employees who have access to enterprise administrative and data systems (e.g., M-Pathways) | Online: <a href="MyLinc">Access and Compliance: Handling Sensitive Institutional Data at U-M</a> | Mandatory 1-time before access is granted; Periodic afterwards as appropriate | ITS/Information Assurance                |
| U-M employees who have access to Protected Health Information               | HIPAA (unit specific)                                                   | Annual                           | UMHS Compliance/UMHS Chief Compliance Officer |
| U-M employees conducting human subject research                             | Online: [Human Subject Research (PEERRS)] (MyLinc)                       | Every three years                 | UMOR/Research Ethics and Compliance      |
| All personnel (principal investigator, researchers, graduate students, research fellows) listed on Technology Control Plan (TCP) with access to export controlled information | Online: <a href="CITI">Introduction to Export Compliance: Export Compliance for Researchers</a> | Prior to start of research project identified in TCP | UMOR/Research Ethics and Compliance        |</p>
<table>
<thead>
<tr>
<th>U-M application and software developers</th>
<th>Secure Coding and Application Development</th>
<th>Periodic</th>
<th>Information and Infrastructure Assurance/CISO</th>
</tr>
</thead>
<tbody>
<tr>
<td>U-M employees who come into contact with credit card data and merchant contacts</td>
<td>Online: <a href="MyLinc">TME102 Merchant Certification Course</a></td>
<td>Annually</td>
<td>U-M Treasurer’s Office</td>
</tr>
<tr>
<td>Information Assurance Staff</td>
<td>Degrees in information assurance; professional certifications including: CISSP; CIPP; CISM; CRISC: CISA, GIAC</td>
<td></td>
<td>CISO</td>
</tr>
</tbody>
</table>

**VI. Implementation**

Information and Infrastructure Assurance is responsible for the implementation, maintenance and interpretation of this Standard.

**VII. References**

- [Safe Computing website](#)
- NIST, Building an Information Technology Security Awareness and Training Program, [NIST SP 800-50 (October 2003)](#)