



Information Technology Services Information Security Office

100 Morrissey Boulevard, Boston, MA 02125

Information Security Training and Awareness Policy

I. PURPOSE

This policy aims to outline the program that will be implemented to ensure effective and active knowledge transfer regarding the University of Massachusetts Boston's (the University) information security policies and to provide security awareness training for the University Community. Faculty, staff, students, and part-time employees (the Community) who have access to the University's information systems must understand how to protect the **confidentiality, integrity, and availability** of these systems. The University acknowledges that cybersecurity is not merely a technical challenge but also a human one. The Program consists of a structured roadmap that enables the University to:

- Reduce human-related security risks.
- Demonstrate program effectiveness through metrics.
- Institute a security-aware culture.

II. SCOPE

It is the University's responsibility to maintain an ongoing information security awareness and training program (the Program) for the Community. The University Information Security Office (ISO) will develop and uphold the Program (**Appendix A**) to educate the Community about information security policies and procedures, ensure they understand their roles and responsibilities in safeguarding information resources, and promote a culture of security. All faculty, staff, students, and part-time employees are required to participate in the program, **complete the annual mandatory cybersecurity training**, be knowledgeable about information security policies and practices, and comply with the procedures and instructions provided in the training.

Security awareness should be ingrained in the University's culture. The community must perceive cybersecurity as a **shared responsibility** and actively support the Program's initiatives. The success of the program relies on utilizing metrics to assess and manage human risk.



This policy encompasses all University information resources, irrespective of how they are managed (individually, shared, stand-alone, or networked). These resources include, but are not limited to, networked devices, cloud computing services, mobile devices (including components), personal computers, workstations, related peripherals and software, and hardcopy information.

III. POLICY

Information systems security and stability are essential for daily operations. A community awareness and training program is crucial for establishing and sustaining a strong information security program. Information security awareness, training, and education will enhance individual behavior and accountability, thereby reducing the risk of unauthorized activities.

All new employees must complete a cybersecurity session during orientation. Human Resources will notify the ISO of all new hires before their orientation date. Additionally, **all members of the University community are required to complete mandatory security awareness training annually**. After each training session, the University will keep records that it deems appropriate to verify that each employee has received adequate training.

The program's primary goal is to create and uphold appropriate protection for data and information resources by enhancing users' awareness of their information security responsibilities. Specific objectives include:

- Raising awareness of the importance of safeguarding information resources.
- Ensuring that users clearly understand their roles and responsibilities in protecting information resources.
- Ensuring that users are familiar with the University's information security policies and practices while equipping them with the skills and knowledge necessary to perform their duties securely.
- Ensuring that users are informed about the laws governing data privacy and regulated data, such as FERPA and HIPAA, as they relate to their job responsibilities.

Training can be provided through various methods (**Appendix A**), both in person and online.

The Chief Information Security Officer (CISO) is responsible for overseeing the development, implementation, and management of the IT Security Training and Awareness Program. Supervisors must ensure that all employees under their supervision complete the necessary cybersecurity training promptly. Adhering to this policy is crucial for maintaining the University's security posture and protecting its information resources.

Functional department managers responsible for managing information resources must receive adequate training on properly implementing security controls for the systems and data they control.

Information technology personnel responsible for administering security controls must receive adequate training on procedures related to security administration.



IV. RESPONSIBILITIES

Role	Responsibility
CISO	<ul style="list-style-type: none"> Manages the development, implementation, and ongoing administration of the Program. Ensures that all members of the Community receive job-specific security training tailored to their roles and responsibilities. Maintains accurate and up-to-date records of training participation and completion.
HR Management Supervisors	<ul style="list-style-type: none"> Ensure that all employees receive appropriate training and fully understand their responsibilities in adhering to and implementing the University’s Information Security Policies. Enforce compliance through disciplinary measures as necessary.
Staff	<ul style="list-style-type: none"> Complete mandatory annual security training as a minimum requirement. Review, fully understand, and commit to adhering to all University Information Security Policies and Guidelines.

V. REFERENCES

Frameworks	Name	Reference
	The Center for Internet Security Controls (v8.1)	CIS 14: Security Awareness and Skills Training; CIS 17: Incident Response Management; CIS 18: Penetration Testing
Regulations and Requirements	N/A	
Supporting Standards and Procedures	N/A	

VI. REVISION HISTORY

Revision Number	Date	Name	Description
20-R1	6/30/2020	UMB-ISTAP-ISOPOL05-20-R1	First Version
25-R1	02/15/2025	UMB-ISTAP-ISOPOL05-25-R1	
(Next Rev.) 21-R1	06/30/2026		



APPENDIX A

INFORMATION SECURITY AWARENESS PROGRAM

The Information Security Awareness Program is offered through various channels, which may include, but are not limited to:

1. ISO provides a mandatory annual cybersecurity awareness and training module.

2. ISO maintains an Information Security website.

The University Information Security Office (ISO) maintains a website showcasing the latest information security announcements, blogs, concepts, best practices, advisories, and relevant security newsletters and articles: <https://www.umb.edu/it/security>

3. ISO offers required cybersecurity training during orientation for new employees.

4. **ISO offers personal strategies for cybersecurity and cyber hygiene.**

The Information Security Office (ISO) offers customized cybersecurity training that focuses on strategies and digital safety protocols tailored to meet individual needs. These sessions highlight practical, sustainable cyber hygiene practices designed to enhance personal digital security, including mindful adjustments to personal devices and effective responses to phishing and other online threats, yielding immediate and significant results.

5. **ISO conducts a comprehensive Cybersecurity Awareness Month (CAM).**

Daily activities during October are structured around annual themes set by the National Initiative for Cybersecurity Careers and Studies (NICCS) and the Cybersecurity and Infrastructure Security Agency (CISA). These themes offer focused frameworks for promoting cybersecurity awareness and best practices across the organization.

6. ISO curates and publishes quarterly newsletters.

In collaboration with IT Communications, the ISO curates and publishes a quarterly newsletter that can be found here: <https://www.umb.edu/it/security>

7. IT Communications sends weekly alerts with IT updates and news, delivering essential cybersecurity information, directives, and announcements from the ISO to the entire Community through mass email.

8. ISO runs frequent simulated phishing campaigns supplemented by mandatory online training for those who fall for phishing.

9. Regulated data compliance awareness training.

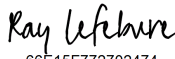


In collaboration with the Information Security Office (ISO), the Registrar's Office provides specialized training on regulated data for employees who manage sensitive information, including but not limited to HIPAA, FERPA, and PII. This training ensures compliance with applicable regulations and promotes secure data handling practices.


- 10. The President's Office controller provides Payment Card Industry (PCI) compliance awareness to individuals handling PCI-related data.

Signature Page

APPROVED BY:

<small>DocuSigned by:</small>	
	2/14/2025
<small>66E46F772702474...</small>	
Raymond Lefebvre	Date
Vice-Chancellor and Chief Information Officer	

APPROVED BY:

<small>DocuSigned by:</small>	
	2/14/2025
<small>668B0E1CEA4540D...</small>	
Wil Khouri	Date
Assistant Vice-Chancellor and Chief Information Security Officer	