University of CINCINNATI	*Policy Title:* **Information Security Awareness, Training, and Education**	*Policy Number:* **9.1.9**
Category: Information Technology	**Effective Date:** April 29, 2024	**Policy Owner:** VP & CDO, Digital Technology Solutions
Policy applicable for: Faculty, Staff, Affiliates	**Prior Effective Date:** N/A	**Responsible Office:** Office of Information Security

Scope

This policy applies to all University of Cincinnati ("UC" or "University") staff, faculty, and any others having access to one or more UC information systems (collectively referred to as the "University Community.")

Background

The University Community plays an important role in maintaining the integrity of University information systems and data by helping to reduce unintentional errors, unauthorized disclosures, and IT vulnerabilities. It is the responsibility of all members of the University Community to protect the confidentiality, integrity, and availability of UC information systems and data. By participating in information security awareness, training, and education, members of the University Community can learn how best to help reduce the risk of data breaches, maintain compliance with applicable laws, regulations, contractual agreements, and UC rules, policies, and procedures.

Policy

The University offers various information security awareness, education, and training activities, informational and instructional resources, and programs intended to enable members of the University Community to carry out their shared responsibility to protect UC's information systems and data.

Members of the University Community are expected to engage in regular data protection awareness, education, training courses and campaigns in accordance with this Policy and as directed by their respective unit(s).

Supervisors are expected to monitor and manage employees' compliance with information security training expectations.

Minimum Training Expectations

Group	Training	Cadence
All staff and faculty	• Information security awareness	Annual
Research faculty and other individuals identified by the Office of Research required to take information security awareness training	• Information security awareness • Insider threat • Controlled Unclassified Information (CUI) • ITAR/Export Controls	Annual and upon receipt of applicable contract
IT Staff and other high-risk users as determined by responsible University unit	• Information security awareness • Information security policies and procedures • Incident reporting • Insider threat • Privileged access	Annual
Information Security Staff	• Information security awareness • Information security policies and procedures • Incident response • Insider threat • Privileged access	Annual and as determined by Chief Information Security Officer

Contact Information

Office of Information Security 513-558-ISEC(4732) infosec@uc.edu