Ohio Administrative Code

Rule 3337-91-05 Information security.

Effective: May 8, 2019

The version of this rule that includes live linksto associated resources is online at

https://www.ohio.edu/policy/91-005

(A) Purpose

This policy provides a framework to continuously protect and secure Ohio universitys data and information resources and comply with and maintain legal and contractual requirements.

(B) Scope

Ohio university organizational units operating technology resources are responsible for ensuring that the set of components for collecting, creating, storing, processing, and distributing information, typically including hardware and software, system users, and the data itself: (OHIO systems) are managed securely. Users (users) are defined as faculty; staff; student employees; third party agents, and any other authorized university affiliates accessing sensitive data.

Unauthorized use or disclosure of data protected by laws or contractual obligations could cause damages to the university, members of the university community, as well as subject the university to penalties in the form of fines or government sanctions. Examples of such laws or contractual obligations are The Health Insurance Portability and Accountability Act (HIPAA) and payment card industry data security standard (PCI-DSS). To properly manage these risks, users must ensure their electronic devices and any other resources which create, collect, store, transmit, or process information meet minimum information security standards.

The information security office (ISO) will advise and consult key stakeholders involved with the protection of data and assets on critical risk issues, and recommend remediation actions to support the information security risk management program (ISRMP) as defined in policy 91.006

Information security risk management. Ohio system and data owners will be responsible for ensuring that mission critical Ohio systems being maintained by them are adequately assessed for risk and that any identified risks are accepted, mitigated, or transferred.

(C) Policy

ISO will consult with stakeholders to define the information security standards which help support and maintain an adequate information security posture. The information assurance and privacy advisory group will approve new standards under the supervision of the information technology partnership group. Each standard identifies controls required for the data or IT resource, and assigns appropriate security risk levels.

The information security standards apply to all IT data resources owned, leased, operated, provided by, or otherwise connected to university resources. This includes, physical assets such as computers, workstations, external drives, mobile phones, wireless devices, operating systems, software, and applications (free or contracted by the university).

Users are required to apply the appropriate controls to the data and IT resource(s) following this process.

Data owners are responsible for identifying the security level for the data and IT resource following the process in policy 93.001 Data classification. The ISO will provide advice and consultation to assist in compliance. Data owners are responsible for applying the appropriate controls from the information security standards, to the data and IT resource based on the security level. The security level defines the minimum requirements that must be followed by each classification, however, units may require additional controls beyond this policy, as no policy can require controls less than those indicated in this policy.

(D) Enforcement

Ohio users must report non-compliance with any part of this policy to the ISO (security@ohio.edu).

Users who do not comply with this policy or related information security standards may be denied

access to information technology ("IT") resources, as well as be subjected to disciplinary action up to and including termination.

(E) Exceptions

All exceptions to this policy must be formally documented with the ISO prior to approval by the president or delegate. Policy exceptions will be reviewed and renewed on a periodic basis by the ISO.

Request an exception:

Complete Initial Exception Request Form, Policy Exception Template, and Risk Acceptance Form. (https://www.ohio.edu/oit/security)

The version of this rule that includes live linksto associated resources is online at

https://www.ohio.edu/policy/91-005