AUTHENTICATED,
OHIO LEGISLATIVE SERVICE
COMMISSION
DOCUMENT #317792

Ohio Administrative Code

Rule 3337-91-06 Information security risk management.

Effective: August 26, 2024

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

https://www.ohio.edu/policy/91-006

(A) Purpose

The information security risk management program ("ISRMP") is the formal process to manage information security risks to Ohio university ("Ohio") to ensure the confidentiality, integrity and availability of university data and information systems ("Ohio systems"), as outlined in the policy 93.001 "Data classification." The ISRMP serves a strategic role in addressing the constantly evolving information security threat landscape by aligning our information technology practice with the universitys risk tolerance.

(B) Scope

This policy applies to all data created, collected, stored, processed, or transmitted by the university and Ohio systems.

(C) Policy

(1) Ohio systems will be assessed for any risks or threats to the integrity, availability, and confidentiality of data prior to significant changes to Ohio systems, in accordance with the university information security officer role as outlined in policy 93.001 "Data classification."

(2) Assessments will be performed periodically for Ohio systems that store, process, or transmit sensitive data.

(3) Risks identified from an assessment will be mitigated, transferred or accepted by the responsible

business owner as described in policy 93.001 "Data classification."

(4) Residual risks will only be accepted by those person(s) with the appropriate level of authority, based on the level of risk determined by the information security office ("ISO"). Approval authority may be delegated if documented in writing, but ultimate responsibility for risk acceptance cannot be delegated.

Risk Level	Risk Acceptance Responsbility
High	President or delegate
Medium	Deans and adminidtrative officers
Low	Business owner

(5) Each mission critical Ohio system will have a system security plan, prepared using input from risk, security and vulnerability assessments, by the responsible business owner.

(D) Responsibilities

(1) The ISO will provide assessments of risks and recommendations to remediate discrepancies found according to industry specific frameworks, methodologies, or business best practices.

(2) Business 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.

(E) Enforcement

Users, as defined in policy 91.005 "Information security," will report any 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.

(F) Exceptions

All exceptions to this policy must be formally documented with 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 excemption:

Complete initial exception request form: https://www.ohio.edu/security/policy-and-practices/standards

(G) Authority

Policy 91.005 "Information security."

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

https://www.ohio.edu/policy/91-006.