Ohio Administrative Code

Rule 3337-91-03 Acceptable usage.

Effective: August 26, 2024

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

https://www.ohio.edu/policy/91-003.html

(A) Purpose

The Ohio university information technology systems ("Ohio systems") incorporate all electronic communication, information systems and equipment used by the university. This acceptable usage policy ("AUP") sets forth the standards by which all users may use the shared campus-wide network ("Ohio network"). The term "users" is defined in policy 91.005 "Information security."

Ohio systems are provided to support the university and its primary objectives towards education, service, and research. Anything that jeopardizes the security, availability, or integrity is prohibited.

By using or accessing Ohio systems, users, agree to comply with the AUP, as well as all other applicable university policies, including all federal, state, and local laws and regulations. Only authorized users may access the Ohio systems, as well as any services interconnected with it.

(B) Scope

Users interacting with Ohio systems, data, identities, and accounts used to access Ohio systems, the Ohio network, and any university data.

(C) Policy

(1) Users may not impersonate another person, organization, or system, including university name, Ohio network names, or Ohio network address spaces.

(2) Users may not attempt to intercept, monitor, forge, alter, or disrupt another users communications or information.

(3) Users may not infringe upon the privacy of others systems or data.

(4) Users may not read, copy, change, or delete another users data or communications without the prior express permission of the other user.

(5) Users may not use Ohio systems in any way that:

(a) Disrupts; impacts the security posture; or interferes with the legitimate use of any computer; the Ohio network or any network to which the university connects.

(b) Interferes with the functions of any system owned or managed by the university, or,

(c) Takes action that is likely to have such effects. Such conduct includes: hacking or spamming; placing of unlawful information on any computer system; transmitting data; or programs likely to result in the loss of an individuals work or result in system downtime; or any other use that causes congestion of any networks or interferes with the work of others.

(6) Users may not distribute or send unlawful communications of any kind. This provision applies to any electronic communication distributed or sent within the Ohio network or to other networks while using the Ohio network.

(7) Users may not attempt to bypass network security mechanisms, including those present on the Ohio network, without the prior express permission of the owner of that system. The unauthorized gathering of information regarding systems or devices on the Ohio network (i.e. network scanning) is also prohibited. Before running any type of network scan, and to obtain authorization, users should contact the information security office ("ISO") for more information.

(8) Users may not engage in the unauthorized copying, distributing, altering or translating of copyrighted materials, software, music or other media without the express permission of the copyright holder or as otherwise allowed by law.

(9) Users may not extend or share with public or other users the Ohio network beyond what has been configured accordingly by the office of information technology ("OIT") and ISO. Users are not permitted to connect or change any network-related infrastructure, devices, or systems (e.g., switches, routers, wireless access points, VPNs, firewalls, virtual or bare-metal) to the Ohio network without advance notice and consultation with OIT and ISO.

(10) Users are responsible for maintaining and deploying minimum levels of security controls on any personal computer equipment connecting to the Ohio network, including but not limited to: antivirus software (with frequent updates), current system patches, and the usage of strong passwords to access these systems as defined in NIST series publications.

(11) Users may not use Ohio systems to violate any laws, regulations, or ordinances.

(D) Responsibilities

All users will be expected to:

(1) Behave responsibly and show respect to the Ohio network and other users at all times.

(2) Respect the security and integrity of Ohio systems, and university data.

(3) Be considerate of the needs of other users by making every reasonable effort not to impede the ability of others to use the Ohio systems and show proper judgement regarding the consumption of shared resources.

(4) Respect the rights and property of others, including privacy, confidentiality, and intellectual property.

(5) Cooperate with the university to investigate potential unauthorized and/or illegal use of the Ohio network.

(E) Enforcement

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

Users who do not comply with this policy or related university information security standards may be denied access to information technology ("IT") resources, as well as be subjected to disciplinary action.

(F) Exceptions

All exceptions to this policy must be approved by the responsible business owner, and be formally documented. Policy exceptions will be reviewed and renewed on a periodic basis by ISO.

Request an exception:

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

(G) Governance

This policy will be reviewed by the ISO and other key stakeholders in the security of university assets and data, to ensure continued compliance, as deemed appropriate based on fluctuations in the technology landscape, and/or changes to established regulatory requirement mandates.

(H) Authority

Policy 91.005 "Information security"

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

https://www.ohio.edu/policy/91-003.html