3358:11-6-01 Information technology policy.

(A) Purpose. Owens community college provides information technology resources to support the academic, administrative, instructional, research and business operations of the college. The purpose of this rule is to maintain and protect the confidentiality, integrity, and availability of the college's information technology resources.

(B) Application. This rule and accompanying standards and procedures are applicable to all information technology devices owned by the college, to any device obtaining connectivity to the college network, and to all relevant data on such devices.

(C) Responsibility.

(1) All users of information technology resources are responsible for reading, agreeing and abiding to this rule.

(2) All users of information technology resources are responsible for practicing safe computing and must use and protect data in a manner consistent with all relevant standards and procedures of information technology services and the rules of the college.

(3) A user of information technology resources must notify college officials upon discovery if an assigned information technology resource has been accessed, attempted to be accessed, or is vulnerable to access by an unauthorized user.

(4) All users of information technology resources are responsible for activity resulting from their assigned information technology resources.

(5) All users of information technology resources must be aware of and comply with all applicable federal, state and other applicable laws, contracts, regulations and licenses, including but not limited to:

(a) United States Code, including but not limited to:

(i) Digital Millennium Copyright Act, Pub. L., No. 105-304, 112 Stat. 2860 (1998), 17 U.S.C. 101

(ii) Electronic Communications Privacy Act of 1986, Pub. L., No. 99-508, 100 Stat. 1848, 18 U.S.C. 2510

(iii) Computer Fraud and Abuse Act of 1986, Pub. L., 99-474, 100 Stat. 1213, 18 U.S.C. 1001

(iv) Family Educational Rights and Privacy Act of 1974, Pub. L., 93-380, 88 Stat. 571, 20 U.S.C. 1232g

(v) Health Insurance Portability and Accountability Act of 1986, Pub. L., 104-191, 110 Stat. 1936, 42 U.S.C. 201

(vi) Gramm-Leach-Bliley Act, Pub. L., 106-102, 113 Stat. 1338 (1999), 12 U.S.C. 1811

(b) Ohio Revised Code, including but not limited to: Section 1349.19 of the Revised Code.

(6) The college must employ reasonable measures to mitigate security threats and will enforce standards and rules to protect college owned or controlled information technology resources.

(7) The college may permit the use of information technology resources for either experimental use or limited social purpose, if it is determined in advance that it will not interfere with institutional operations or violate standards and procedures of information technology services and the rules of the college.

(8) The college may restrict or block any subsidiary application or protocol that becomes a risk to the security of the information technology infrastructure, as deemed appropriate or necessary and without prior notice.

(9) The college prohibits the following actions, including but not limited to:

(a) An attempt or the circumvention of an information technology security system such as a firewall, anti-virus software, encryption, password or by a physical method;

(b) The disruption of college operations such as a configuration of devices that disrupt network service, a launch denial of service attacks or the disturbance to public access of resources;

(c) The use of information technology to conduct reconnaissance, vulnerability assessments, or similar activity by unauthorized personnel;

(d) Anonymous use, impersonation, or use of pseudonyms on an information technology resource to escape accountability; examples include but are not limited to: forging email or the use of any internet service not affiliated with the college that can prevent accountability for its usage;

(e) The use of devices that broadcast any wifi signal is prohibited on any college owned or occupied property, unless it is part of the wireless service being deployed by the college.

(D) Security and privacy statement. Owens community college respects the privacy of all information technology data users. The college does not routinely monitor the content of material but does reserve the right to access and review all aspects of its information technology infrastructure to investigate performance or system problems, search for harmful programs, or upon reasonable cause, to determine if a user is in violation of any college rule, standard or procedures, state or federal laws, contract or license. The college may monitor, keep and audit detailed records of information technology usage; traces may be recorded routinely for troubleshooting, performance monitoring, security purposes, auditing, recovery from system failure, etc.; or in response to a complaint, in order to protect the college's and others' equipment, software and data from unauthorized use or tampering. Extraordinary record keeping, traces and special techniques may be used in response to technical problems or complaints, or for violation of law, rules, standards or regulations, but only on approval by college administration specifically authorized to give such approval. In addition to the privacy of an individual being respected under normal circumstances, the privacy of those involved in a complaint will be respected, and the college will limit special record keeping in order

to do so, where feasible. Information will be released in accordance with law. Users should be aware that while the college implements various security controls to protect information technology resources, protection of data from unauthorized individuals cannot be guaranteed.

(E) Non-compliance. Non-compliance with this rule and corresponding procedures may be subject to the Owens community college rule 3358:11-5-52 of the Administrative Code (standards of conduct and disciplinary process policy and corresponding procedures) or the college's student code of conduct. Access privilege may be suspended without prior notice if it is determined that a violation is causing a current or imminent threat to the confidentiality, integrity or availability of information technology resources. Furthermore, failure to abide or comply with applicable federal, state or other applicable law, regulation, contract or license may result in a potential civil or criminal sanction under the law.

(F) Implementation. The treasurer/chief financial officer or the chief information officer has the authority to promulgate procedures, guidelines and forms consistent with this rule.

(G) Effect on prior policy. This rule repeals and supersedes all portions of the Owens community college rule of 3358:11-4-10 of the Administrative Code (responsible computing policy).

(H) All users of information technology resources may reference definitions and standards for the college's information technology services at the following webpage link. https://www.owens.edu/helpdesk/definitions.pdf.

Replaces:	3358:11-4-10
Effective:	12/14/2019

CERTIFIED ELECTRONICALLY

Certification

12/04/2019

Date

Promulgated Under:	111.15
Statutory Authority:	3358.08
Rule Amplifies:	3358.08
Prior Effective Dates:	03/07/2002