Title/Subject: **RESPONSIBLE USE OF COMPUTING**

Applies to: ☒ faculty ☒ staff ☒ students ☒ student employees ☒ visitors ☒ contractors

Effective Date of This Revision: July 1, 2017

Contact for More Information: Office of Information Technology

☐ Board Policy ☒ Administrative Policy ☐ Procedure ☐ Guideline

---

I. POLICY STATEMENT

It is the policy of the University to provide and maintain computing, networking and telecommunications technologies to support the education, research, and work of its student, faculty, and staff. The University respects the rights of users to express their own opinions in their personal communications using the computer systems. To preserve the privacy, availability, and integrity of CMU computing resources, and to protect all users' rights to an open exchange of ideas and information, this policy sets forth the responsibilities of each member of the CMU community relative to the use of these resources. To accomplish these ends, this policy also supports resolution of complaints raised under this policy.

Every user of CMU computing resources must be aware that violations of this policy may result in revocation of access, suspension of accounts, disciplinary action, or prosecution, and that evidence of illegal activity will be turned over to the appropriate authorities. It is the responsibility of each member of the CMU community to read and observe this policy and all applicable laws and procedures. Any violations of this policy should be reported by e-mail to the CMU Security Incident Response Team (CMU-SIRT) at **abuse@cmich.edu** or by phone to the Chief Information Security Officer (CISO) in the Office of Information Technology (OIT) at 989.774.7445 or the OIT Help Desk at 989-774-3662.

With the approval of the appropriate senior officer, areas may add individual guidelines that supplement, but do not change, the intent of these policies.

The computing, networking and telecommunications technologies established or maintained by CMU are the property of CMU, as are any software licenses purchased with university funds. The computer records created or maintained by employees and contained in these systems - including documents, email, listserv archives, text messages, and voice mail - are the property of CMU. Exceptions to CMU ownership of such records include those addressed through grant or contractual relationships with external agencies or those in which ownership rights are transferred through other CMU policies, such as the Intellectual Property Rights Policy. Information concerning the retention of such records is available in the CMU Records Retention schedule at **https://www.cmich.edu/office_provost/OIT/Pages/Record-Retention.aspx**

II. SCOPE AND APPLICABILITY OF THIS POLICY

Anyone using or accessing CMU computers, networks, systems or data is subject to the provisions of this policy. CMU faculty, staff, emeritus faculty and staff, registered students, alumni, and approved guests are permitted to use CMU's computing and networking services, but are subject to the terms of this policy during that use. Individuals who use personally-owned equipment while connected to the university network are subject to the provisions of this policy while

---

Authority: George E. Ross, President
History: Rules for Computing & Networking Resources, 08-28-97; 12-01-08; 09-08-10
Indexed as: Computer Use; Networking; Telecommunication Technologies; Data Use; Privace of Computer Records

connected to the network. Use of CMU's computing and networking facilities and equipment by unauthorized persons is prohibited. Other responsibilities of users are detailed in "Rules of Use" below.

CMU Technical Staff who are specifically hired to maintain CMU's computing and networking resources have special privileges and special responsibilities under this policy. These staff are required to keep confidential any personal information that they come in contact with in the course of performing their duties, but are also required to report any known misuse or abuse of computing and network resources. They have been granted extraordinary powers to override or alter access controls, configurations, and passwords, which they must exercise with great care and integrity. In addition to following the tenets of this policy, CMU Technical Staff are expected to abide by the code of ethics identified and maintained by the SAGE Organization at https://www.usenix.org/sites/default/files/code_of_ethics_poster_english.pdf.
SAGE is a Special Interest Group of the **USENIX Association**, which is the primary professional organization of systems administrators.

The CMU Systems Incident Response Team (CMU-SIRT) is primarily responsible for monitoring the health, integrity, and performance of the CMU network. As these duties overlap this policy, CMU-SIRT is also responsible for reviewing decisions of other OIT staff, responding to complaints, providing security advice, and periodically reviewing this and other information security policies. The CMU-SIRT is appointed by the CIO, is chaired by the CISO, and consists of representatives from multiple areas of OIT, including core technologies, core applications, and other teams. The CMU-SIRT will establish a dispatching procedure for routing complaints to the appropriate official or staff member for action. The CMU-SIRT monitors CMU systems and network activities, coordinates responses to abuses, provides technical assistance on security matters to OIT staff and university administrators, and issues security advisories. The CMU-SIRT is also responsible for periodically recommending improvements and clarifications to this policy to the CISO and CIO.

III. RULES OF USE

Access to CMU computing resources is a privilege granted on a presumption that every member of the University community will exercise it responsibly. Because it is impossible to anticipate all the ways in which individuals can damage, interrupt, or misuse CMU computing facilities, this policy focuses on a few simple rules.

RULE 1: Use of CMU computing resources must be consistent with University priorities.

a) CMU-SIRT will attach greatest priority to uses that support the academic, research, and business functions of the University. Such uses can include web browsing, chat sessions, and personal communications. The use of the network for entertainment purposes constitutes the lowest of its priorities and may be preempted should diversion of resources to a higher priority be deemed necessary. In order to maintain these priorities, the University reserves the right to limit the amount of resources an individual user consumes.

b) A number of actions are specifically forbidden: engaging in illegal peer-to-peer file sharing or other illegal downloading; selling access to CMU computing resources; intentionally denying or interfering with any network resources, including spamming, jamming and crashing any computer; using or accessing any CMU computing resource, or reading or modifying files, without proper authorization; sending chain letters; and engaging in activities prohibited under the terms of the CMU Advocacy Policy or the CMU Solicitation and Fundraising Policy. (See VI. Related Policies below)

RULE 2: Users must not impersonate any other entity and must not allow anyone else to impersonate them.

a) Using CMU computing resources to impersonate someone else is wrong. Access to CMU systems and network using another user's logon credentials is fraudulent and prohibited by this policy. Similarly, mail or postings from CMU systems must not be sent anonymously.

b) Users are required to be responsible for the security and use of their logon credentials. Users agree to take reasonable steps to avoid the negligent disclosure or distribution of security credentials and agree that a failure to do so may represent misconduct for which discipline may be administered. Most CMU systems are designed so that logon credentials create an audit trail for important business processes and security purposes. Sharing, even negligently, logon credentials with others circumvents this vital aspect of system integrity. For this

reason, and to forestall potential abuse, users must keep their credentials private and not allow others to use them. OIT maintains a process for obtaining temporary access to required functionality across its systems. Requests for extended functionality must be directed to the CMU Help Desk at 989.774.3662.

RULE 3: Users must honor the privacy of other users.

a) Personal e-mail, electronic files maintained on University equipment and personal Web pages are part of a comprehensive electronic information environment. This environment creates unique privacy issues that involve federal and state laws as well as University policies.

b) Users have the right to expect that their legitimate uses of computing and networking resources are private. CMU users who invade the privacy of others may have their access suspended and may also be subject to University disciplinary action through appropriate channels. Users must not access the contents of files of another user without authorization from that user.

c) Users must not intercept or monitor any network communications not explicitly meant for them.

d) Users must not create or use programs, hardware, or devices that collect information about other users without their knowledge and consent. Software on CMU computing resources is subject to the same guidelines for protecting privacy as any other information-gathering project at the University. Further, users may not disclose private information that they discover while accessing CMU systems, even if that access is for legitimate use.

RULE 4: Users must not perform any action on the network that in any way threatens the network or any systems or data connected to it.

a) OIT maintains network quotas to support reasonable use, and users must not engage in any activity designed to circumvent these quotas. Users who have extraordinary bandwidth needs should work with OIT to address these needs.

b) Users must not extend the CMU network without explicit permission from OIT. The unauthorized use of routers, switches, modems, wireless access points, and other devices can impact the security and stability of the network and is strictly prohibited. All use of network addresses or other address spaces as contracted by the University must be registered with OIT.

c) Users must not use CMU computing resources to attack computers, accounts, or other users by launching viruses, worms, Trojan horses, or other attacks on computers at CMU or elsewhere.

d) Users must not perform unauthorized vulnerability scans on systems; such scanning is considered to be a hostile act.

e) Because of the rapid pace of technological change, CMU-SIRT has extraordinary powers to interpret this rule and may apply it to any activity not identified here that threatens 1) the health of the CMU network, systems, or applications or 2) the integrity of data including personal information about users.

RULE 5: Users must not use CMU computing resources to commit violations of any law or any published University policy, procedure, guideline, standard, or recommendation.

a) Users must adhere to licensing agreements that the University has with its vendors. As an example, some software installed on University-owned computers is restricted by contract to educational uses by CMU faculty, staff, and students and may not be used for commercial, administrative, or other purposes. CMU has processes in place to verify that software is distributed in compliance with its contractual agreements, and those processes often explicitly ask CMU users to agree to the terms of CMU's license with the vendor. It is always incumbent

on each CMU user, however, to ensure that their use of the software remains in compliance with the CMU license.

b) Possession of a copy of CMU-licensed software does not imply personal ownership or unrestricted use of that software.

c) Users who leave the University must relinquish any university-owned hardware and equipment, any university-licensed software, and, consistent with the University's Intellectual Property Rights Policy, all CMU-owned data. Questions about appropriate use of CMU-licensed software may be directed to the Chief Information Security Officer in the Office of Information Technology at 989.774.7445.

d) Users must not violate copyright laws. Such violations include, but are not limited to, illegal peer-to-peer file sharing and unauthorized downloading of copyrighted content (like movies, songs, TV shows, and other broadcasts).

e) Users must not use CMU computing resources to harass others or to publish libelous statements. Various types of harassment, including sexual or racial, are proscribed by other University policies. (See Related Policies below)

f) Users of CMU computing resources are subject to all federal and state obscenity laws. The use of University resources to access pornographic materials for non-work purposes may result in disciplinary action, up to and including termination.

g) Users must not use CMU email or other technology to send unsolicited commercial email as defined in Michigan's UNSOLICITED COMMERCIAL E-MAIL PROTECTION ACT.

IV. UNIVERSITY ACCESS TO DIGITAL INFORMATION

CMU will exercise its right of access to the digital information of users only in the following circumstances:

a) Those instances where the university has a legitimate "need to know." Examples include those where there is reasonable suspicion that: a user is using email to threaten or harass someone; a user is causing disruption to the network or other shared resources; a user is violating university policies, laws, or another user's rights; a student is engaged in academic dishonesty; or a faculty or staff member is in violation of the university's Research Misconduct Policy. **"Need to know" access will be conducted by OIT staff only after securing the approval of the General Counsel.** If access provides evidence of violation of law, this policy, or other University policies, the results of such access may be shared with other appropriate officials of the University.

b) Those instances in which the university must comply with a Freedom of Information Act request, a subpoena, or a discovery request.

c) Those instances in which an employee is absent from work and access to specific computer records is critical to continue the work of the University during their absence.

d) Those instances in which access to university information is required in order for OIT staff to carry out their administrative practices - e.g., backing up files, cleaning up trash or temporary files, searching for rogue programs, or conducting routine systems maintenance. This restriction does not apply to the collection of audit trails and usage logs by OIT staff. There are times, however, in the regular course of their jobs, when OIT staff may come in contact with private or personally-identifiable information. In this event, OIT staff are responsible

for keeping that information secure and must not divulge it to anyone unless they believe a breach of law or policy has occurred. OIT staff are regularly reminded of this responsibility.

V. RELATED POLICIES

Advocacy Policy

Solicitations and Fundraising Policy

Workplace Violence Policy

Information Security Policy

Data Stewardship Policy

Affirmative Action Protocol

Sexual Misconduct Policy

VI. COMPLIANCE

a) Incidents that violate this policy may or may not require an immediate response. Those that pose immediate danger to persons, systems, or property will be addressed by the appropriate university agencies. Whether or not an incident requires immediate response, violations of this policy may result in revocation of access, suspension of accounts, disciplinary action, or prosecution. Evidence of illegal activity will be turned over to the appropriate authorities.

b) New users will be asked to indicate their agreement to this policy as a condition of activating their accounts and registering their computers for use on the CMU network.

VII. AMENDMENTS AND ADDITIONS

The CIO may approve exceptions to this policy. All substantive amendments and additions to this policy will be drafted by a committee convened by the CIO and will be reviewed and approved by the Provost and the President. Changes in this policy will be appropriately publicized.