Acceptable Use Policy for MSU Information Technology Resources

Administrative Ruling – January 27, 2012

A trusted and effective information technology environment ("IT environment") is vital to the mission of Michigan State University. To that end, the university provides an IT environment which includes an array of institutional electronic business systems, computing services, networks, databases, and other resources (collectively, "MSU IT resources" or "resources"). These resources are intended to support the scholarship and work activities of members of the university's academic community and their external collaborators, to support the operations of the university, and to provide access to services of the university and other publicly available information.

Access to and usage of MSU IT resources entails certain expectations and responsibilities for both users and managers of the IT environment. These are stated below.
()

I. Applicability

1.1. This Policy applies to all individuals using MSU IT resources ("Users"), regardless of affiliation and irrespective of whether these resources are accessed from MSU's campus or from remote locations.

1.2. Within MSU's IT environment, additional rules may apply to specific computers, computer systems or facilities, software applications, databases and data sources, data types, or networks, and to the uses thereof, or to local workplaces, or to specific types of activities (collectively, "local rules"). Local rules must be consistent with this Policy, but also may impose additional or more specific requirements or responsibilities on Users.

1.3. Users will be notified of, or given ready access to (e.g., on a website), this Policy and local rules that govern use of MSU IT resources.
()

II. Purposes & Appropriate Uses

2.1. MSU IT resources are provided for university-related purposes, including support for the university's teaching, research, and public service missions, its administrative functions, and student and campus life activities.

2.2. Users are granted access to MSU IT resources for the purposes described in this Policy. Use should be limited to those purposes, subject to Section 2.3.

2.3. Incidental Personal Use

2.3.1. Users may make incidental personal use of MSU IT resources, provided that such use is subject to and consistent with this Policy, including Article 3 of this Policy. In addition, incidental personal use of MSU IT resources by an MSU employee may not interfere with the fulfillment of that employee's job responsibilities or disrupt the work

environment. Incidental personal use that inaccurately creates the appearance that the university is endorsing, supporting, or affiliated with any organization, product, service, statement, or position is prohibited.

2.3.2. Users who make incidental personal use of MSU IT resources do so at their own risk. The university cannot guarantee the security or continued operation of any MSU IT resource.
()

III. User Responsibilities

3.1. Users are responsible for informing themselves of any university policies, regulations, or other documents that govern the use of MSU IT resources prior to initiating the use of MSU IT resources.

3.2. Use of Resources Accessed through MSU IT Resources

3.2.1. When using MSU IT resources or resources owned by third parties that are accessed using MSU IT resources, Users must comply with all applicable federal and state laws, all applicable university rules, ordinances, and policies, and the terms of any contract or license which governs the use of the third-party resource and by which the User or the university is bound.

3.2.2. In amplification and not in limitation of the foregoing, Users must not utilize MSU IT resources to violate copyright, patent, trademark, or other intellectual property rights.

3.3. Users may not engage in unauthorized use of MSU IT resources, regardless of whether the resource used is securely protected against unauthorized use.

3.4. Privacy of Other Users

3.4.1. Users are expected to respect the privacy of other Users, even if the devices and systems by which other Users access MSU's IT resources, the content other Users place on MSU IT resources, or the identities and privileges (rights to access and use certain systems and/or data), of other Users are not securely protected.

3.4.2. Unauthorized use by a User of another User's personal identity or access (login) credentials is prohibited.

3.5. MSU IT resources have a finite capacity. Users should limit their use of MSU IT resources accordingly and must abide by any limits MSU places on the use of its IT resources or on the use of any specific IT resource. In particular, no User may use any IT resource in a manner which interferes unreasonably with the activities of the university or of other Users.

3.6. MSU IT resources may not be used to fundraise, advertise, or solicit unless that use is approved in advance by the university.

3.7. Partisan Political Activities

3.7.1. MSU IT resources may not be used to engage in partisan political activities on behalf of, or in opposition to, a candidate for public office.

3.7.2. MSU IT resources may not be used to promote or oppose the qualification, passage, or defeat of a ballot question that does not affect the university's interests. MSU IT resources may not be used to promote or oppose the qualification, passage, or defeat of a ballot question that affects the university's interests unless that use is approved in advance by the President.

3.7.3. These prohibitions do not apply to private devices that are attached to the university's network, provided that MSU IT resources are not used in a way that suggests the university endorses or supports the activity originating on the private device.

3.8. MSU IT resources may not be used to operate a business or for commercial purposes unless that use is approved in advance by the university.

3.9. MSU IT resources may not be used to support the operations or activities of organizations that are not affiliated with the University unless that use is approved in advance by the university.

3.10. Pornography and Sexually Explicit Content

3.10.1. Unless such use is for a scholarly or medical purpose or pursuant to a formal university investigation, Users may not utilize MSU IT resources to store, display, or disseminate pornographic or other sexually explicit content. This prohibition does not apply to private devices that are attached to the university's network.

3.10.2. Child pornography is illegal. The use of MSU IT resources to store, display, or disseminate child pornography is absolutely prohibited. Any such use must be reported immediately to the MSU Police Department.

3.11. In operating its IT environment, the university expects Users to engage in "safe computing" practices, such as establishing appropriate access restrictions for their accounts, setting strong passwords and guarding those passwords, keeping their personal operating systems and software applications up-to-date and patched, and employing security measures on their personal devices.
()

IV. Enforcement

4.1. Use of MSU IT resources is a privilege and not a right. A User's access to MSU IT resources may be limited, suspended, or terminated if that User violates this Policy. Alleged violations of this Policy will be addressed by the Chief Information Security Officer of IT or his/her designee.

4.2. Users who violate this Policy, other university policies, or external laws may also be subject to disciplinary action and/or other penalties. Disciplinary action for violation of this Policy is handled through the university's normal student and employee disciplinary procedures.

4.3. In addition to its own administrative review of possible violations of this Policy and other university policies, the university may be obligated to report certain uses of MSU IT resources to law enforcement agencies. (See e.g., Section 3.10.2.)

4.4. If the Chief Information Security Officer determines that a User has violated this Policy and limits, suspends, or terminates the User's access to any MSU IT resource as a result, the User may appeal that decision to the Chief Information Officer (CIO). If the User believes that his/her appeal has not been appropriately addressed by the CIO, he/she may seek further redress as follows:

4.4.1. if an undergraduate student, through the Vice President for Student Affairs, or his/her designee;

4.4.2. if a graduate or professional student, through the Dean of the Graduate School, or his/her designee;

4.4.3. if a member of the faculty or academic staff, through the Associate Provost and Associate Vice President for Academic Human Resources, or his/her designee;

4.4.4. if an employee covered by a collective bargaining agreement, through the Director of Employee Relations, or his/her designee.

4.5. Alleged violations of local rules will be handled by the local systems administrator, network administrator, or employee supervisor/unit manager, depending on the seriousness of the alleged violation. These individuals will inform and consult with the Chief Information Security Officer or his/her designee regarding each alleged violation of a local rule and the appropriate consequences for any violation of a local rule. Users who object to the limitation, suspension, or termination of their access to any MSU IT resource as a consequence of their violation of a local rule may appeal to the CIO.

4.6. The CIO may temporarily suspend or deny a User's access to MSU IT resources when he/she determines that such action is necessary to protect such resources, the university, or other Users from harm. In such cases, the CIO will promptly inform other university administrative offices, as appropriate, of that action. Local MSU IT resource administrators may suspend or deny a User's access to the local resources they administer for the same reasons without the prior review and approval of the CIO, provided that they immediately notify the Chief Information Security Officer and the CIO of that action.
()

V. Security & Operations

5.1. The university may, without further notice to Users, take any action it deems necessary to protect the interests of the university and to maintain the stability, security, and operational effectiveness of its IT resources. Such actions may be taken at the institutional or local level, and may include, but are not limited to, scanning, sanitizing, or monitoring of stored data, network traffic, usage patterns, and other uses of its information technology, and blockade of unauthorized access to, and unauthorized uses of, its networks, systems, and data. Local and central institutional IT resource administrators may take such actions in regard to the resources they manage without the prior review and approval of the CIO as long as the actions involve automated tools and not direct human inspection.
()

VI. Privacy

6.1. General Provisions

6.1.1. Responsible authorities at all levels of the MSU IT environment will perform management tasks in a manner that is respectful of individual privacy and promotes User trust.

6.1.2. Monitoring and Routine System Maintenance

6.1.2.1. While the university does not routinely monitor individual usage of its IT resources, the normal operation and maintenance of those resources requires the backup of data, the logging of activity, the monitoring of general usage patterns, and other such activities. The university may access IT resources as necessary for system maintenance, including security measures.

6.1.2.2. The university's routine operation of its IT resources may result in the creation of log files and other records about usage. This information is necessary to analyze trends, balance traffic, and perform other essential administrative tasks. The creation and analysis of this information may occur at central institutional and local levels.

6.1.2.3. The university may, without further notice, use security tools and network and systems monitoring hardware and software.

6.1.3. The university may be compelled to disclose Users' electronic records in response to various legal requirements, including subpoenas, court orders, search warrants, discovery requests in litigation, and requests for public records under the Michigan Freedom of Information Act ("MIFOIA").

6.1.4. The university reserves the right to monitor and inspect Users' records, accounts, and devices as needed to fulfill its legal obligations and to operate and administer any MSU IT resource.

6.1.5. The university may disclose the results of any general or individual monitoring or inspection of any User's record, account, or device to appropriate university authorities and law enforcement agencies. The university may also use these results in its disciplinary proceedings.

6.2. Provisions Regarding Inspections and Disclosure of Personal Information

6.2.1. General provisions:

6.2.1.1. In order to protect User privacy, the CIO or his/her designee must review and approve *any* request for access by a person to an individual User's personal communications or electronically stored information within MSU IT resources.

6.2.1.2. Incidental access to the contents of an individual User's personal communications or electronically stored information resulting from system operational requirements described elsewhere in this Policy does not require the prior review and approval of the CIO.

6.2.2. The university, acting through the CIO, may access or permit access to the contents of communications or electronically stored information:

6.2.2.1. When so required by law. If necessary to comply with the applicable legal requirement, such disclosures may occur without notice to the User and/or without the User's consent.

6.2.2.2. In connection with an investigation by the university or an external legal authority into any violation of law or of any university policy, rule, or ordinance. When the investigational process requires the preservation of the contents of a User's electronic records to prevent their destruction, the CIO may authorize such an action.

6.2.2.3. If it determines that access to information in an employee's electronic account or file is essential to the operational effectiveness of a university unit or program and the employee is unavailable or refuses to provide access to the information.

6.2.2.4. If it receives an appropriately prepared and presented written request for access to information from an immediate family member or the lawful representative of a deceased or incapacitated User.

6.2.2.5. If it must use or disclose personally identifiable information about Users without their consent to protect the health and well-being of students, employees, or other persons in emergency situations, or to preserve property from imminent loss or damage, or to prosecute or defend its legal actions and rights.

Revised June 5, 2017, to change "Vice President for Information and Technology and CIO" to "CIO."

Revised June 13, 2016, to change "Deputy CIO" to "Chief Information Security Officer" and"CIO and Director of Information Technology" to "Vice President for Information Technology and CIO."

Revised June 13, 2013, to change "Vice Provost for Libraries and IT Services" and "VPLITS" to "CIO and Director of Information Technology."

Revised June 20, 2012, to change "Vice Provost for Libraries, Computing and Technology" and "VPLCT" references to "Vice Provost for Libraries and IT Services" and "VPLITS." Also changed "Director of Academic Technology Services" and "ATS" references to "Deputy CIO of IT Services" and "IT Services."

Acceptable Use Policy Outline

Every Spartan has a duty to protect personal and institutional data. Stay cyber secure. (http://secureit.msu.edu/)

MICHIGAN STATE
UNIVERSITY
(http://www.msu.edu)

Call us: **(517) 432-6200**