6.02 - INFORMATION TECHNOLOGY USAGE

Effective: August 1, 2025

Purpose: The purpose of this policy is to outline the acceptable uses of computing and information technology resources at Emporia State University.

Scope: This policy applies to faculty, staff, students, official University affiliates, and any other individual who uses University computing and information technology resources.

Responsible Office: Information Technology

Policy Statement: The Chief Information Officer (CIO) will be responsible for:

- Determining and posting operational policies, networking standards and procedures in consultation with University governing bodies so as to implement the principles outlined in this policy.
- Reviewing and updating this policy in consultation with the relevant University governance structure.
- Monitoring and reporting compliance with this policy.

Information Technology (IT) has the responsibility to protect shared information technology services. In the event of hardware or software failure, or in the event of an attack by malicious user(s), designated IT staff will quarantine any technology resources necessary to solve the problem, to protect the system or systems connected to the network, and the information the system contains.

The ISO is responsible for working with IT and Unit Support personnel to implement a network logon banner using the Logon Banner Standards.

Authorized users of University computing and information technology resources are responsible for reviewing and following published Information Security policies and procedures.

Use of University Information Technology Resources

It is University policy to provide computing and information technology resources to faculty, staff, students, official University affiliates, and others in support of the education, research, and public service missions of the University.

Users of University computing and information technology resources are responsible for using these resources only as allowed by law and in connection with the University's core teaching, research, service, and other identified missions. Users must abide by the following standards of acceptable use:

- Users shall abide by applicable state and federal laws, all University and Board of Regent policies, and all applicable contracts and licenses.

- Each user is responsible for the activities that occur while they are using the computing and technology resources assigned to them and will use only those resources for which the individual has authorization and only in the manner and extent authorized.
- Users shall respect the copyright and intellectual property rights of others and ensure the legal use of copyrighted material.
- Users shall use computing and information technology resources in a manner that does not interfere with, compromise, or harm the University's technology resources.

Uses of University computing and information technology that do not significantly consume resources or interfere with other users may also be acceptable but may be restricted by Information Technology (IT) upon advice of the University President, or their designee. Under no circumstances shall members of the University community or others use University information technology resources in ways that are illegal, that threaten the University's tax-exempt status, or that interfere with reasonable use by other members of the University community.

Examples of inappropriate or unauthorized use of University IT resources include but are not limited to:

- Using electronic information resources, including email, messaging, and web pages, to illegally discriminate against, harass, defame, or threaten individuals or organizations;
- Engaging in illegal conduct or conduct that violates University policy;
- Destruction of or damage to equipment, software, or data belonging to others;
- Disruption or unauthorized monitoring of electronic communications;
- Interference with use of University systems;
- Circumvention of computer security systems;
- Unauthorized use of accounts, access codes, or identification numbers;
- Use that intentionally impedes the legitimate computing activities of others;
- Use for commercial purposes or for personal gain to include Cryptocurrency mining;
- Use for political or lobbying activities that jeopardize the University's tax-exempt status and, therefore violates University policy;
- Violation of copyrights, software license agreements, patent protections and authorizations, or protections on proprietary or confidential information;
- Unauthorized use of University trademarks;
- Violating copyright laws by downloading and sharing files;
- Violations of privacy;
- Academic dishonesty;
- Sending chain mail;
- Spamming;
- Downloading, viewing, and/or sharing of materials in violation of University policy regarding unlawful activity;

- Intrusion into computer systems to alter or destroy data or computer programs (e.g., hacking or cracking);
- Sending communications using campus email or messaging that attempt to hide the identity of the sender or represent the sender as someone else; or
- Engaging in cyberbullying against any individual or organization

Access to University computing and information technology resources requires appropriate permission and access to resources is not guaranteed. The extension of these privileges is predicated upon the user's acceptance of and adherence to the corresponding user responsibilities detailed in this policy and other applicable policies and laws. Activity that violates the conditions set forth in this policy will be investigated as a security event. The University reserves the right to grant, limit, or revoke access to information technology resources without prior notice in order to protect university resources.

Use of Artificial Intelligence (AI) Tools

- Users must not use AI tools in a manner that violates academic integrity, copyright laws, or university policies.
- AI-generated content must be clearly attributed and used in accordance with applicable academic and research standards.
- The use of AI for decision-making that affects individuals (e.g., grading, hiring, or disciplinary actions) must be approved by the appropriate university authority.
- AI tools must not be used to generate or disseminate misinformation, deepfakes, or content that could harm the university's reputation or operations.
- Use of generative AI tools must comply with data privacy and security standards, especially when handling sensitive or regulated data (e.g., FERPA, HIPAA).

Return of IT Assets Upon Termination

- All university-owned computing devices, software licenses, data storage devices, and access credentials must be returned or revoked upon termination of employment, enrollment, or affiliation.
- Departing users must not retain or transfer university data to personal devices or accounts.
- IT will conduct an exit audit to ensure all digital and physical assets are accounted for and access to university systems is terminated.
- Failure to return university assets may result in legal or disciplinary action.

Confidentiality and Privacy

Communications made using University computing and information technology resources are considered to be non-confidential communications. There is no expectation of privacy regarding such communications, which may be subject to access and disclosure under the Kansas Open Records Act (KORA). Confidential information should not be sent using email transmissions unless encrypted using a University supplied encryption product. Examples of such confidential information include but are not limited to records and data subject to the Family Educational Rights and Privacy Act (FERPA) and implementing regulations.

In general, information stored on University owned equipment and resources will be treated as confidential. However, the user of University owned equipment should have no expectation of personal privacy or confidentiality of documents and messages stored on University owned equipment and resources. Additionally, information stored on University networks may be accessed by the University for purposes related to security management, security operations, and legal compliance.

Reporting Violations

Users and administrative or academic units will report any discovered unauthorized access attempts or other improper usage of University computing and technology resources to the Chief Information Officer (CIO), the Information Security Officer (ISO), or other appropriate administrator as per the Information Security Incident Reporting Procedures.

Consequences for Violations

Persons in violation of this policy are subject to the full range of sanctions, including but not limited to, the suspension of system privileges.
At the time, if disciplinary procedures are initiated, in accordance with published policies and rules of conduct, the person alleged to be in violation of the policy will be notified of the alleged violation.

Suspension of system privileges for students may also be handled according to the procedures outlined in the Student Code of Conduct.

In all cases, information will be disclosed as required by controlling law.

Definitions: All words and phrases shall be interpreted utilizing their plain meanings unless otherwise defined in another University or Board of Regents policy or by statute or regulation.

Procedures: All procedures linked and related to the policies above shall have the full force and effect of policy if said procedures have first been properly approved by the University's administrator in charge of Information Technology.

[Hyperlink to Information Technology procedures]

Related Policy Information: [Include here any supporting information for this policy]

History: Adopted: 05/08/2006 [FSB 05010 passed by Faculty Senate on 04/18/06, approved as interim policy by President and included in UPM as Policy 3J.03]
Revised: 12/11/2009 [Revised interim policy approved by the President]
Revised: 03/10/2010 [FSB 09010 passed by Faculty Senate on 03/2/2010 and approved by President]

Revised: 10/02/2013 [Policy Updated]
Revised: 02/18/2020 [Policy removed from Faculty Senate]
Revised: 03/04/2020 [Policy revised by IS and approved by ISAC]
Revised: 08/15/2024 [Policy format revised as part of UPM Revision]
Revised: 08/01/2025 [Policy updated]