K-State home » Policies » PPM » 3400 Computing and Information Technology » PPM Chapter 3420: Information Technology Usage Policy

Policies

Information Technology Usage Policy

Chapter 3420

Revised/Reviewed: September 2, 2010, July 29, 2020, June 9, 2021, August 9, 2022

Table of Contents

.010 Overview and Purpose

This document constitutes a University-wide policy for the appropriate use of all University computing and network resources. This policy is subject to all applicable laws and regulations. It is intended to reflect industry standards with regard to data security, technology, and intellectual property (IP) protection and to ensure compliance with local, state, and federal requirements. It is also intended to complement the other University policies on information technology usage and data security. See PPM 3400-3495 (/policies/ppm/3400/index.html).

.020 General Policy

Access to K-State networks and computer systems is granted subject to University and Kansas Board of Regents policies and local, state, and federal laws.

It is the responsibility of each individual who has access to K-State networks and computer systems to ensure that their activity will not intentionally have a negative impact on the confidentiality, integrity, or availability of all

K-State computing and network resources.

The University is not responsible for inappropriate or unethical use of the information technology environment, including networks and computer systems.

Policy violations shall be reported (see section .070 Reporting Violations) (#report).

.030 Appropriate Use

Authorized users are:

- All provisioned eID holders, including those who have been granted a special access eID (see the K-State eID Policy, PPM Chapter 3450 (/policies/ppm/3400/3450.html)).
- Anyone connecting from a public information service.
- Others whose access furthers the mission of the University and whose usage does not interfere with other users' access to resources.

In addition, a user must be specifically authorized to use a particular computing or network resource by the campus unit responsible for operating the resource.

Appropriate use of University IT resources shall:

- Be for the purposes of furthering the mission of the University.
- Be for the purposes for which they are assigned.
- Be in accordance with all license and contractual agreements to which the University is a party.
- Not install or use peer-to-peer software or software commonly used for unauthorized acquisition or distribution of copyrighted or licensed material on university computers or those attached to the university network.
- Comply with policies of any network over which such data or information must be routed to reach its final destination.
- Not interfere with the operation of University IT resources nor unreasonably interfere with the appropriate use of University IT resources by other users.
- Not indirectly violate this policy by using any device, software, or services of another network provider to circumvent the intent or meaning of this policy.
- Not compromise the security and confidentiality of data that is the property of University or any other user of University IT resources.
- Not attempt to circumvent or subvert any system's security measures.
- Not represent yourself electronically as another user.
- Not disrupt services, damage files, or intentionally damage or destroy equipment, software, or data belonging to the University or other users.
- Not be for personal purpose other than incidental and minimal use.
- Not be for private commercial use unless authorized by contract.
- Not intentionally misrepresent personal identity.
- Be in accordance with state and federal laws (includes such laws as FERPA, Gramm Leach Bliley Act, DMCA (Digital Millennium Copyright Act), US copyright laws, and policies regarding the protection of data).
- Not conflict with or violate any other University or Kansas Board of Regents policy.

.040 Confidentiality and Privacy

While the University does not routinely monitor individual usage of its computing resources, the University may monitor the activity and access the accounts of individual users of University computing resources, including individual login sessions and communications, without notice, for any University purpose; there is no expectation of privacy for users. Some examples of monitoring and access include, but are not limited to:

A. The user has given permission or has voluntarily given access, for example, by posting to a publicly-accessible web page or providing publicly-accessible network services.

B. It reasonably appears necessary to do so to protect the integrity, security, or functionality of the University or other computing resources or to protect the University from liability.

C. There is reason to believe the user has violated, or is violating, this or any University policy.

D. An account appears to be engaged in unusual or unusually excessive activity, as indicated by the reviewing of general activity and usage patterns.

E. Normal operation and maintenance of the University's computing resources require the backup and caching of data and communications, logging of activity, reviewing of general usage patterns for the unauthorized disclosure of institutional data, scanning of systems and network ports for anomalies and vulnerabilities, and other such activities that are necessary to render service or to meet University legal obligations.

F. It is otherwise required or permitted by law.

Any such monitoring or access must be authorized in advance by the Chief Information Officer (CIO) or the Chief Information Security Officer (CISO). The CIO or CISO will work with the appropriate Cabinet-level administrator(s), and/or President before giving approval to proceed.

The University, in its discretion, through the CIO or CISO, may disclose the results of any such general or individual monitoring and information accessed, including but not limited to the contents and records of individual communications, to appropriate University personnel, and/or in reporting to appropriate authorities. The University also may use those results in University disciplinary proceedings and as the University otherwise deems necessary. Additionally, communications made by means of University computing resources are generally subject to the Kansas Open Records Act to the same extent as they would be if made on paper.

.050 Responsible Use of Library-provided Electronic Content

Electronic content made available by the K-State Libraries is provided through specific license agreements. These licenses describe who can use the resource, how it may be used, and the consequences of misuse. Excessive or systematic downloading may result in denial of access. While definitions differ, publishers generally consider multiple sequential chapters of a book or more than half of an entire issue of a journal excessive. Many licenses limit the use of materials to authorized users. Authorized users are K-State faculty, staff, and currently enrolled students. Sharing electronic resources with non-authorized users is prohibited. Sharing passwords, placing licensed materials on a publicly accessible website, and commercial use of licensed information is prohibited. Use of any Library electronic resources constitutes acceptance of K-State’s Information Technology Usage Policy, PPM Chapter 3420.

.060 Training

Annual cybersecurity and data protection training is provided for all users and mandatory for all K-State employees.

.070 Reporting Violations

All users and units shall report unauthorized access attempts or other violations of this policy on K-State computers, networks, or other information processing equipment. If a user observes or learns of a security or abuse problem with any University computer or network facilities, including violations of this policy, the user should notify the Chief Information Officer (CIO), or the Chief Information Security Officer (CISO).

.080 Sanctions

Persons in violation of this policy are subject to the full range of sanctions, including but not limited to the loss of computer or network access privileges without notification, disciplinary action, dismissal from the University, and legal action. Some violations may constitute criminal offenses, as outlined in Kansas statutes and other local, state, and federal laws; the University will report such violations to the appropriate authorities.

Unit heads have the authority to deny access, for unauthorized use, to K-State's network and computer systems under their control.

.090 Questions

Questions regarding this policy should be sent to the Vice President for Information Technology and Chief Information Officer (CIO) (mailto:its@k-state.edu) or the Chief Information Security Officer (CISO) (mailto:security@k-state.edu?subject=).