Acceptable Use Policy (ISP-02)

Document Owner

Executive Owner:	Darrell Morrison
Functional Area:	Information Technology

Authorization

Authorized By:	David J. Hinson
Position:	Interim Chief Information Officer
Signature	
Authorization Date	02/25/2025

Version History

Issue	Reason For Change	Date
1.0	Initial Release	02/25/2025

Review Period

Information Security Policies are to be reviewed at a minimum annually.

Change Control

Requests for changes to Information Security Policies are to be sent to the document owner providing details of the requested changes and a short justification.

Exceptions

Requests for exceptions to this policy are to be submitted in accordance with the exception policy. Note that all exceptions are time limited to no more than 12 months in duration.

Applicability

This policy applies to all faculty, staff, students, and contractors who are issued access to University Information Systems, resources, services, data and networks.

Table of Contents

Introduction

Acceptable Use Policies have been shown to be an effective mechanism for ensuring users of IT systems are aware of their personal responsibilities to secure and protect University Information Systems and data. Additionally, they outline what Users may do and what they may not do when using University Information Systems, and finally they lay out what monitoring and oversight Users must expect.

Objective

The Objective of this policy statement is to ensure all Users are made aware of their responsibilities when utilizing University provided IT, network, systems and services to perform work, educational and personal activities. Thereby protecting users from illegal or damaging actions by individuals, either intentionally or unintentionally

Definitions

Information Systems - Include IT systems, computers, devices, networks and data held on the same.
Users - include students, staff, faculty and contractors who access or make use of University Information Systems and networks.

Policy Statement

General

The University is responsible for securing its Information Systems (both academic and administrative) against unauthorized access, while making the systems accessible for legitimate academic and administrative purposes. This responsibility includes informing persons who use the University Information Systems of the expected standards of conduct and encouraging their adoption. Furthermore, effective security is a team effort involving the participation and support of every User of University assets.

It is the responsibility of every User to know and understand the policy guardrails defined in this document, and to conduct their activities accordingly. The University expects Users to act and behave in an ethical manor when performing computing activities to ensure they do not adversely affect the work and welfare of other individuals and entities.

Data held on University Information Systems, except for personal identifiable information (PII), remains the sole property of the University.

All users should understand that the University is unable to guarantee the protection of electronic files, data or e-mails from unauthorized or inappropriate access.

Monitoring

Users of the University's Information Systems should be aware that use, activity and content will be

subject to monitoring and logging and may be subject to review or disclosure as part of a legal order, for IT security and miss use investigations, and as otherwise required to protect the reasonable interests of the University and other users of the computer system. Anyone using the University's Information Systems expressly consents to monitoring on the part of the University for these purposes and is advised that if such monitoring reveals possible evidence of criminal activity, University administration may provide that evidence to law enforcement officials.

Monitoring audit and investigation will include all Information Systems including but not limited to email, chat, telephony, file transfers and the like. Only the CISO or Legal counsel can authorize reviews of User email and IM chat traffic. All audits, reviews and investigations will be conducted in compliance with federal and state law, as well as appropriate university policies and procedures.

Services, data and applications including file shares and cloud storage may be backed up to other media by the University IT Department for Data Protection measures.

Statement of Use

Users of University Information Systems are responsible for the following:

1. Using only the computer ID assigned to them. Under no condition are Users to share account IDs and passwords with other Users, individuals or administrators. The only exception to this is for the purpose of sharing User passwords on initial account fulfilment or reset. Under those conditions systems are to be programmed to require an immediate reset of the password.
2. University owned devices are to be physically secured when not within immediate reach of the User.
3. University provided Information Systems cannot be used for non-University work such as private consulting, commercial enterprise and/or for personal financial gain.
4. Using University Information Systems for occasional personal use, be that for email, shopping watching video feeds or playing computer games is permitted, but the use should be proportional and only during break or nonworking time for employees and contractors. Users are responsible for exercising good, sound judgment in such use.
5. Staff, faculty, and contractors are to take extreme care in how they communicate with external bodies and entities over electronic mechanisms, particularly when using social media. In simple terms unless you are a direct report to the President or a member of the Communications and Marketing team you are not to express a view in a way that it could be misconstrued as being University view or policy.
6. Users are not to download software from external sources to any University owned device or system without written permission of the IT Department.
7. Users are to ensure they do not intentionally or unintentionally send out mass unsolicited email on campus unless they have been explicitly authorized to do so.
8. Users should avoid initiating any computing and/or transmission intense activities which would degrade system performance during peak periods.
9. Users shall not supply or attempt to supply false or misleading information or identification in order to access computer systems or networks.
10. Users shall not attempt to subvert the restrictions associated with any computer accounts.
11. Use of OneNet, Southern Regional Education Board (SREB), and other systems to which the University connects and /or is associated, shall be governed by the policies and guidelines of said service.

If assistance is needed interpreting and defining what is or is not “Acceptable Use”, Users should contact the Information Technology Helpdesk at extension 884 or helpdesk@ecok.edu., or their supervisor, or faculty counselor for guidance.

Obscenity Law and the Internet

Users must not use University Computing Systems to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace policies, local, state, or federal laws. Oklahoma has adopted the "Miller test" (Miller vs. California, 1973) and has attached criminal penalties to obscene expression. The Miller test provides the following definitions of obscenity:

- Whether the average person, applying contemporary community standards would find that the work, taken as a whole, appeals to the prurient interest:
- Whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law: and
- Whether the work, taken as a whole, lacks serious literary, artistic political or scientific value;

Federal law prohibits conduct similar to that at the state level. The general federal restriction on obscenity is codified at 18 U. S. C. S. 1461-1465.

Information Systems may not be used as an instrument to intimidate or offend people. Using the computer as a means of communication to terrify, intimidate, threaten, harass, annoy or offend another person. Use of a computer as a means of communicating indecent, lewd or obscene language to another person, or communicating a threat or lewd suggestion to another person, shall be prima face evidence of intent to terrify, intimidate, threaten, harass, annoy or offend.

University Web Page Creation and Content

Web pages that contain University data on admissions, grants, programs and similar are to adhere to the Office of Marketing and Communications standard. All such pages are to be reviewed by that office prior to release to ensure technical integrity and protection of the University's image.

Capacity Constraints

The University may from time to time impose capacity limits on system use and at that time it is the Users responsibility to manage within that capacity. Once use exceeds 95% of the capacity, a notice will be sent requesting that the user archive or delete content. Once the 100% limit is reached, system use will be constrained or terminated.

Procurement of Information Services

The IT Director is to approve the procurement of all Information Services, including Devices, Network capacity, Applications and Software. They are to work with the IT Security team to ensure a secure configuration standard is developed and deployed to reduce the attack surface prior to deployment of the same.

Use of Personal or Non-University Devices

Staff, faculty and contractors are normally prohibited from processing Restricted and Confidential data on Information Systems not owned by the University. The only exception to this is for those participating in the Bring Your Own Device program in compliance with that policy. In detail the following non-University provided Information Systems are prohibited from use for all University Business:

- USB, SD cards and other external storage devices
- Cloud storage other than that procured and allocated by the University
- Personal or non-University provided email
- Messaging applications such as WhatsApp and IMessage

1. Social media unless approved by IT Security and Communications and Marketing teams

Theft of Devices and Services

Theft of physical and logical services can be a crime under state and federal law. Violators will be referred to the appropriate University and or External agency for disciplinary action. Accounts may be subject to immediate deactivation.