Information Security Policy (ISP-01)

Document Owner

Executive Owner:	Darrell Morrison
Functional Area:	Information Technology

Authorization

Authorized By:	David J. Hinson
Position:	Interim Chief Information Officer
Signature	
Authorization Date	06/23/2025

Version History

Issue	Reason For Change	Date
1.0	Initial Release	06/23/2025

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 IT resources and services known as Information Systems.

Table of Contents

Document Owner 1
Authorization 1
Version History 1
Review Period 1
Change Control 1
Exceptions 1
Applicability 1
Table of Contents 2
Introduction 3
Objective 3
Definitions 3
Policy Statement 3
- General 3
- Applicable Policy Statements 3
- Location of Policy Documents 4

Failure to Comply 4

Introduction

East Central University of Oklahoma ("University") has adopted this Information Security Policy as a mechanism for defining the steps we all must take in configuring, maintaining, and using University Information Systems to protect the confidentiality, integrity and availability of our Information Systems. Information Security is everyone's responsibility. The security of the University's and your personal data is reliant on how you use the system, how our administrators and faculty use the system and how our IT department and vendors build and maintain our systems.

Objective

The objective of this master policy is to list the constituent policy statements and identify who they apply to in order that you can easily and efficiently navigate the content.

Definitions

University is used throughout the policy series as an abbreviation for the East Central University of Oklahoma

Users are defined as students, staff, faculty, employees, contractors, partners, and any other person authorized to access and use the University's Information Systems.

Information Systems are defined as the IT systems, applications, networks, devices, services, and information contained in them; that transmit and process University data either on the University premises or in third party or cloud provider facilities.

Policy Statement

General

The CIO is to ensure that these IT Security Policies are reviewed at least annually and on major change to IT security controls.

Applicable Policy Statements

The table below lists the constituent policy statements which when combined define the Information Security Policy for the University. With the goal of ensuring policy statements are targeted at specific Users with the University we have identified the target audience in the applicability column.

Users are to review the Policies applicable to themselves and ensure they are compliant. If you have questions about these policies, you should first discuss the issue with your supervisor, manager or student counselor and escalate to the Director of Information Technology.

Ref	Policy Name	Applicability
ISP-01	Master Information Security Policy	All faculty, staff, students, and contractors
ISP-02	Acceptable Use	All faculty, staff, students, and contractors
ISP-03	Access Control	IT, HR and admissions staff and contractors
ISP-04	Risk Management	IT and IT security, systems owners
ISP-05	Inventory Management	IT and Finance department staff and contractors
ISP-06	Password	All faculty, staff, students, and contractors
ISP-07	Encryption	Staff and contractors who administer IT systems
ISP-08	Data Classification and Retention	IT staff and Data Stewards
ISP-09	Change Management and logging	Staff and contractors who administer IT systems
ISP-10	Data Protection and backup policy	Staff and contractors
ISP-11	Wireless Use Policy	All faculty, staff, students, and contractors
ISP-12	Security Awareness Training	All faculty, staff, students, and contractors
ISP-13	Bring Your Own Device (BYOD)	All faculty, staff, students, and contractors
ISP-14	IT Security Incident Response	Staff and contractors who administer IT systems
ISP-15	Exception	Faculty, staff, and contractors

It should be noted that in addition to the security policies the University maintains a Privacy policy in compliance with FERPA student privacy requirements that can be found here:

https://www.ecok.edu/policies-and-handbooks/ecu-family-educational-rights-and-privacy-act-ferpa-1974-and-related-policies.php

Location of Policy Documents

All policy documents can be found at:

https://ecok.edu/policies-and-handbooks/information-security-polices.php

Failure to Comply

Failure to comply with the Policy statements may result in disciplinary action up to and including termination of employment or student rights. Disciplinary action for violating the policy shall be governed by, but not be limited to, the applicable provisions of student handbooks, faculty and staff handbook, policies of East Central University, Board of Regents of Oklahoma Colleges, Oklahoma State Regents for Higher Education, Statutes of the State of Oklahoma, and federal law. In the case of contractors and vendors this may result in your personal or your company's contract being cancelled.

Additionally, Users who violate this policy may also have their access privileges to ECU computing and networking systems revoked.