



Policy Number: VI.01
Policy Level: Operating Policy
Originally Issued: October 9, 2013
Revised: April 13, 2016
Revised: November 16, 2016
Revised: March 7, 2017
Revised: April 1, 2019
Reviewed: August 17, 2021
Reviewed: December 4, 2023
Revised: February 13, 2026
Policy Owner: Chief Information Officer
Policy Implementation: Chief Information Officer
SACSCOC Standard: 10.6

Information and Communication Technologies Acceptable Use Policy

I. Purpose and Scope

This policy defines acceptable and unacceptable use of University information and communication technologies (ICT) to protect University systems, data, and users; to meet legal, regulatory, and contractual obligations; and to support the University's mission. It applies to all users (students, faculty, staff, contractors, vendors, guests) and all University ICT resources, whether on premises or premises or cloud. University technology resources are provided to support academic, administrative, and operational missions thus must be used responsibly, ethically, and lawfully.

II. Ownership, Privacy, and Monitoring

All content and activity on University ICT are subject to monitoring, access, and disclosure by authorized University officials for business, operational, legal, and security purposes, with or without notice, and may be shared with law enforcement where appropriate. Users should have no expectation of privacy when using University ICT, except where required by law.

III. Responsibilities

Users must comply with this policy and report suspected security incidents, phishing, or lost/stolen devices immediately through designated channels.

Supervisors ensure users under their direction understand this policy and complete required security awareness training.

CIO/Information Security Officer develops and maintains procedures/standards supporting this policy and coordinates incident response.



Policy Number: VI.01
Policy Level: Operating Policy
Originally Issued: October 9, 2013
Revised: April 13, 2016
Revised: November 16, 2016
Revised: March 7, 2017
Revised: April 1, 2019
Reviewed: August 17, 2021
Reviewed: December 4, 2023
Revised: February 13, 2026
Policy Owner: Chief Information Officer
Policy Implementation: Chief Information Officer
SACSCOC Standard: 10.6

IV. Acceptable Use

Use University ICT primarily for University-related teaching, research, learning, and administration. Limited incidental personal use is permitted if it does not interfere with business operations, incur additional cost, or violate law or policy.

V. Prohibited (Unacceptable Use)

- Share passwords or use another person's account; create, use, or maintain unauthorized or shared accounts.
- Attempt to gain unauthorized access, circumvent security controls, or conduct "hacking," port scanning, traffic capture, or similar activities without written authorization.
- Introduce or distribute malware; send mass unsolicited messages; spoof identities; or engage in phishing, social engineering, or fraudulent activities.
- Store, process, or transmit sensitive University data without required protections or approvals (e.g., encryption in transit/at rest, approved storage locations).
- Use ICT to create, access, or share content that is threatening, defamatory, obscene, harassing, discriminatory, or otherwise unlawful; or that violates intellectual property or license terms.
- Connect unauthorized devices or services to the University network or cloud tenants, including rogue wireless access points, network taps, or personal hotspots used to bypass controls.



Policy Number: VI.01
Policy Level: Operating Policy
Originally Issued: October 9, 2013
Revised: April 13, 2016
Revised: November 16, 2016
Revised: March 7, 2017
Revised: April 1, 2019
Reviewed: August 17, 2021
Reviewed: December 4, 2023
Revised: February 13, 2026
Policy Owner: Chief Information Officer
Policy Implementation: Chief Information Officer
SACSCOC Standard: 10.6

VI. Minimum Security Expectations for Users

- Strong Authentication. Users must comply with University MFA and password requirements where applicable (e.g., remote access, administrative access, externally exposed apps).
- Data Handling. Users must classify, store, share, and retain data per University data-handling standards; encrypt sensitive data in transit and at rest where required.
- Email & Web Safety. Do not bypass University protections (e.g., DNS filtering, URL filtering, anti-malware, DMARC). Report suspected phishing and other suspicious ITC activities.
- Awareness & Training. Complete security awareness training at hire and annually; additional role-based training as assigned.

VII. Third Parties and Service Providers

Vendors, contractors, and other service providers with access to University ICT or data must comply with this policy and applicable security requirements in their contracts (e.g., incident notification, encryption, secure disposal).

VIII. Reporting, Investigation, and Cooperation

Users must promptly report suspected security incidents via the University's designated reporting channels. The University may isolate devices/accounts during investigations and will coordinate responses consistent with the Incident Response Plan.



Policy Number: VI.01
Policy Level: Operating Policy
Originally Issued: October 9, 2013
Revised: April 13, 2016
Revised: November 16, 2016
Revised: March 7, 2017
Revised: April 1, 2019
Reviewed: August 17, 2021
Reviewed: December 4, 2023
Revised: February 13, 2026
Policy Owner: Chief Information Officer
Policy Implementation: Chief Information Officer
SACSCOC Standard: 10.6

IX. Exceptions

Exceptions to this policy require documented business justification, risk assessment, and written approval by the CIO (or designee). Time-bound exceptions must be reviewed and renewed or retired.

X. Enforcement

Violations may result in suspension of ICT privileges, disciplinary action (up to termination/expulsion), restitution for damages, and referral to law enforcement.

XI. Responsibility for this Operating Policy

Policy Owner

As part of the initial approval of this policy by the President and subsequent to the original dissemination of the policy, the Chief Information Officer is the policy owner for the ongoing evaluation, review, and approval of this policy. Subsequent reviews and revisions to this policy must be in accordance with approved operating policy procedures and processes.

This policy will be reviewed every two years or more frequently as needed by the Policy Owner. Revisions will be reviewed/affirmed by the Cabinet and approved by the University President. This policy will be updated/published in the University's Policy Library.

Responsibility for Policy Implementation

The President has assigned the responsibility of implementing this policy to the Chief Information Officer.