4-OP-H-21 Acceptable Use of Technology Policy

Responsible Executive: Finance and Administration

Approving Official: Vice President for Finance and Administration

Effective Date: March 1, 2024

Revision History: No revisions at this time.

I. INTRODUCTION

A. PURPOSE

The purpose of this policy is to define acceptable use of Florida State University (FSU) Information Technology (IT) resources. Users are required to comply with all applicable federal, state, and local laws, and FSU policies and supplemental **standards (https://its.fsu.edu/cybersecurity/standards)** in their use of FSU's IT resources.

Appropriate use of FSU's technology resources reduces the risk of unauthorized access and modification of information, theft of intellectual property, exposure of personal or private information, and risks to data and infrastructure that affect continuous operations.

B. SCOPE

This policy applies to all users and their use of FSU IT resources and services, whether accessed by FSU-owned or personal devices. IT resources and services include all hardware and software that access or store FSU data, conduct FSU business, or interact with internal networks and business systems.

Individual university units or organizations may define additional conditions, restrictions, or guidelines for their communities that are consistent with FSU IT policies and standards.

C. DEFINITIONS

IT Glossary (https://its.fsu.edu/sites/g/files/upcbnu4396/files/1ITS Website 2023/Documents/Cybersecurity/File_Cybersecurity_IT_Glossary_202303.pdf)

D. ROLES AND RESPONSIBILITIES

It is the responsibility of authorized users to comply with this policy.
The University Chief Information Officer (CIO) and the Chief Information Security Officer (CISO) are responsible for implementing this policy and ensuring the operation of the University's IT resources is consistent with laws and other university policies.

For more information, see **IT Roles and Responsibilities (https://its.fsu.edu/cybersecurity/standards/it-roles-and-responsibilities)**.

II. POLICY

A. ACCESS AND USE OF UNIVERSITY SYSTEMS AND INFORMATION

Access to FSU IT resources is provided in support of academic and research activities, as well as for reasonable and appropriate personal use. Personal devices can pose risks to the university environment (e.g., data leakage, malware introduction, unauthorized access). Members of the FSU community must protect and secure personal devices used on the FSU network or that access university information. Personal devices must not be used to access or download university information classified as

High Risk or Moderate Risk, as defined by the **4-OP-H-25.01 Data Security Standard (https://its.fsu.edu/cybersecurity/standards/data-security-standard)**. For use and access to be acceptable, all users must protect the security and integrity of information and IT resources through their compliance with:

- applicable federal, state, and local laws as they relate to IT resources
- all FSU IT policies and supplemental standards
- safe computing practices, including compliance with required password protection as defined by the **4-OP-H-25.07 IT Access, Authorization and Authentication Standard (https://its.fsu.edu/cybersecurity/standards/it-access-authorization-and-authentication-standard)**
- respect for the privacy and personal rights of others
- proper handling and safekeeping of records as defined by **4-OP-F-3 Records Management (https://policies.vpfa.fsu.edu/policies-and-procedures/records-information/records-management)**.

In accordance with Florida law, FSU blocks access to prohibited applications, websites, and technologies on university devices or personal devices while using FSU's Wi-Fi, virtual private network, and any network FSU owns, operates, or maintains.

Prohibited applications are defined as those that:

- are created, maintained, or owned by a foreign principal and that engage in specific activities that endanger cybersecurity; or
- present a security risk in the form of unauthorized access to or temporary unavailability of a public employer's information technology systems or data, as determined by the Department of Management Services (DMS).

B. **PROTECTING DATA AND RESOURCES**

Approved FSU Technologies and Applications

Only technologies and applications reviewed and approved for use by Procurement Services, Office of the General Counsel, and the Information Security & Privacy Office may be used. Technologies and applications provided by ITS (see **Services | Information Technology Services (https://its.fsu.edu/services)** or third-party vendors under formal agreement with FSU to ensure security and privacy protections are approved for use.

Examples of Inappropriate Use of University Systems

1. Unauthorized Use
    - any activity that could potentially disable, alter, or circumvent network or device security measures, such as imposing an exceptional load on IT resources (e.g., email spamming, network denial of service)
    - any activity which may adversely affect the confidentiality, integrity, or availability of IT resources or data
    - unauthorized or impersonating the use of systems
    - exhibiting a pattern of malicious network traffic scanning or attacking others
    - unapproved access or viewing of pornography (unless necessary and approved in writing by the CUU and University Unit DDDH for academic

instruction or research)

  - creating, processing, storing, or utilizing information classified as High Risk or Moderate Risk on any systems other than those approved by ITS
  - deleting or destroying public records without authorization

2. Failure to Adhere to University Polices

  - any activity that interferes with job performance or responsibilities
  - any activity that results in additional cost to FSU or is inconsistent with FSU’s not-for-profit status
  - use of unapproved systems, applications, and technologies such as unapproved email systems for conducting university business
  - using unapproved applications (e.g., Facebook, GroupMe, Discord, YouTube, etc.) for instruction or course administration that violate FSU privacy policies
  - any use of a university account for personal gain or to solicit others for personal financial gain (e.g. the use of Canvas to solicit the sale of class notes, study guides, textbooks, apartment leases, etc.)

3. Failure to Adhere to Laws

  - Illegal activities, such as violations of intellectual property and copyright infringement
  - engaging in activities that harasses, threatens, or abuses others
  - federal, state, and local computer security violations
  - failure to properly safeguard personal information in accordance with privacy laws (e.g. the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”))
  - bomb threats and hoaxes
  - child pornography and distribution of pornography to minors. Suspected violations will be reported to the FSU Police Department and other appropriate law enforcement entities immediately

University units may implement additional limits on personal use of University IT beyond the parameters of this policy. Any additional limits must be documented and communicated to users and the Information Security and Privacy Office (ISPO).

C. **POLICY VIOLATIONS AND INCIDENT REPORTING**

Failure to comply with the requirements of this policy or supplemental policies and standards may result in reduced or revoked access to network and other IT resources.

FSU may remove a website or other document or information from any FSU server if found to be in violation of federal, state, or local laws or rules or FSU rules, policies, or procedures.

Users who violate this policy may be subject to other penalties and disciplinary action, both within and outside FSU. Disciplinary action is governed under FSU's standards for disciplinary action for violation of provisions of University policy and applicable student conduct codes.

Unauthorized or fraudulent use of university computing resources may result in criminal prosecution.

Incidents occur when an FSU student, staff, contractor, or faculty member violates this policy, specific legal requirements, or contractual obligations. It is the responsibility of each FSU student, staff, contractor, or faculty member to immediately report suspected or confirmed Information Security and Privacy Incidents to the Chief Information Security Officer (CISO) at **security@fsu.edu (mailto:security@fsu.edu)**. The CUU ISM, University Unit ISM, or Inspector General must inform the CISO of any suspected or confirmed incidents within 24 hours. Refer to the **4-OP-H-25.11 IT Incident Response Standard (https://its.fsu.edu/cybersecurity/standards/it-incident-response-standard)** for more information.

Refer to the **<4-OP-H-30 Health Information Portability and Accountability Act (HIPAA) Policy>** if a HIPAA security incident or breach is suspected or confirmed.

D. **EXCEPTIONS TO POLICY AND STANDARDS**

Exceptions for any provision of this policy or supplemental IT Standards must be approved in accordance with the **4-OP-H-25.20 Request for Exception to IT Security Policy (https://its.fsu.edu/cybersecurity/standards/request-exception-it-security-policy)**.

Any questions regarding the requirements of this Policy or supplemental IT Standards should be referred to ISPO at 850-644-HELP or via the Contact information at **https://its.fsu.edu/. (https://its.fsu.edu/.)**

E. **RELATED POLICIES, STANDARDS AND DOCUMENTS**

Standards | Information Technology Services (https://its.fsu.edu/cybersecurity/standards)

External Apps Supported in FSU's Canvas (https://support.canvas.fsu.edu/kb/article/772-external-apps-supported-in-fsus-canvas/)

4-OP-F-3 Records Management (https://policies.vpfa.fsu.edu/policies-and-procedures/records-information/records-management)

ITS Supported Services (https://its.fsu.edu/service-catalog/All-Services)

IT Security and Privacy Incident Response and Reporting Procedures (http://security.fsu.edu/content/download/173837/1512697/FSU Incident Response and Reporting Procedures August 1 2014.pdf)

External Apps Supported in FSU's Canvas (https://support.canvas.fsu.edu/kb/article/772-external-apps-supported-in-fsus-canvas/)

III. **LEGAL SUPPORT, JUSTIFICATION, AND REVIEW OF THIS POLICY**

SPECIFIC AUTHORITY

Chapter 119, Florida Statutes (https://www.flsenate.gov/Laws/Statutes/2019/Chapter119) - Public Records

BOG Regulation 3.0075 (https://www.flbog.edu/wp-content/uploads/3_0075SecurityofDataandRelatedITResourcesFINALformat.pdf) - Security of Data Related Information Technology Resources

Chapter 501.171, Florida Statutes (http://www.leg.state.fl.us/Statutes/index.cfm?App_mode=Display_Statute&URL=0500-0599/0501/Sections/0501.171.html) – Security of Confidential Personal Information, Florida Information Protection Act 2014 (FIPA)

Family Educational Rights and Privacy Act (FERPA) (https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html)

Health Insurance Portability and Accountability Act (HIPAA) (https://www.hhs.gov/hipaa/index.html)

Payment Card Industry Data Security Standard (PCI DSS) (https://www.pcisecuritystandards.org/pci_security/)

Federal Information Security Modernization Act (FISMA) (https://www.cisa.gov/federal-information-security-modernization-act)

Chapter 282.318, Florida Statutes (https://www.flsenate.gov/Laws/Statutes/2019/282.318) - Information Technology Security Act

Florida Information Protection Act (FIPA) (https://www.flsenate.gov/Session/Bill/2014/1524)- Security of Confidential Personal Information

Gramm Leach Bliley Act (http://www.business.ftc.gov/privacy-and-security/gramm-leach-bliley-act)

The Federal Trade Commission (FTC) Rule on "Standards for Safeguarding Customer Information" (https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/safeguards-rule)

CHAPTER 2023-32 "An act relating to prohibited applications on government-issued devices" (https://laws.flrules.org/2023/32)

SUS Prohibited Technologies List (https://www.flbog.edu/wp-content/uploads/2023/04/SUS-Prohibited-Technologies-List-4-2023-1.pdf)