FVSU Acceptable Use Policy

1. **Reason for Policy**

Fort Valley State University's (FVSU) Acceptable Use Policy (AUP) provides the guiding principles for the use of Information Technology (IT) Resources at FVSU. It is expected that all users of FVSU IT resources will use them responsibly and to the benefit of the mission of FVSU. Appropriate use of FVSU IT Resources allows the University to achieve its academic and research missions while maintaining a culture of openness, trust, and integrity within our digital spaces.

2. **Policy Statement**

University IT Resources must be used in accordance with applicable licenses and contracts, and according to their intended use in support of the University's mission. All users must comply with federal, state, and local laws, as well as FVSU policies when using FVSU IT Resources. Fort Valley State University requires all users of all USG Information Technology (IT) resources and services to conduct themselves responsibly. Users must respect the public trust that provides the resources; comply with federal, state, and local laws; comply with USG policies, standards and directives; respect the rights and privacy of others; and respect the integrity of USG facilities and controls. The following sections define the acceptable uses of FVSU IT Resources.

3. **Scope**

All FVSU IT resource users are covered by this policy. This policy applies to all users, including institutions, employees, students, contractors, guests, vendors, and any other authorized person or organization ("users"), of all USG Information Technology (IT) resources and services. IT resources and services include but are not limited to hardware, software, networks, data, the internet when accessed through USG resources, and communication systems, whether owned, leased, or otherwise provided by USG organizations ("resources").

4. **Acceptable Use**

4.1. Employees and Student Employees Excluding incidental personal use, as defined below, FVSU IT Resources must be used only to conduct the legitimate business of the University (e.g., scholarly activity, academic instruction, research, learning, and business operations).

- **Incidental Personal Use:** Incidental personal use of FVSU IT Resources by FVSU employees is permitted if the personal use does not interfere with the execution of job duties, does not incur cost on behalf of the University, and is not unacceptable as defined in the Unacceptable Use section below.

4.2. Students FVSU students may use the campus network for recreational and personal purposes to the extent that such use is not unacceptable as defined in the Unacceptable Use section below and does not adversely affect network service performance for other users engaged in academic, research, or official business activities.

5. Unacceptable Use

FVSU employees, including students acting as employees, are prohibited from the following actions when using FVSU IT Resources. All users are prohibited from using FVSU IT resources in a manner that results in a violation of law or policy or potentially adversely affects network service performance. Examples of Unacceptable Use include, but are not limited to, the following:

- Activity that violates federal, state, or local law.
- Activity that violates any University or Board of Regents policy.
- Activities that lead to the destruction or damage of equipment, software, or data belonging to others or the University.
- Circumventing information security controls of University IT Resources.
- Releasing malware or intentionally installing malicious software.
- Impeding or disrupting the legitimate computing activities of others.
- Unauthorized use of accounts, access codes, passwords, or identification numbers.
- Unauthorized use of systems and networks.
- Unauthorized monitoring of communications not intended for you without permission or in support of official duties.
- Unauthorized use of IT Resources for commercial purposes or personal gain.
- Transmitting commercial or personal advertisements, solicitations, or promotions.
- Using unauthorized third-party software or information services to store, access, or process USG information.
- Transmitting, disseminating, selling, storing or hosting material on USG resources that is unlawful, libelous, defamatory, obscene, pornographic, harassing, threatening, abusive or invasive of privacy rights.
- Storing protected or confidential information in unintended or unprotected locations.
- Using unsupported or expired software in violation of USG guidelines.
- Downloading, using, or distributing copyrighted materials without permission.
- Downloading, using, or distributing pirated software, music, videos, or games.
- Making or using more copies of licensed software than permitted.

This list is not complete or exhaustive. It provides examples of prohibited actions. Any user in doubt about the acceptable use of FVSU IT Resources should contact the

Office of Information Technology for further clarification and assistance.

6. Mobile Workforce (Personally Owned Devices - PODs) Requirements

Although USG IT service providers are charged with preserving the integrity, confidentiality, availability and security of USG managed data and information resources, security may be compromised through actions beyond any user's control. Personally Owned Devices (PODs) used by any user presents a special risk to USG resources because device owners install and configure software applications, security settings and perform their own maintenance and may share the device with others. If PODs are permitted to access USG IT resources, the user authorizing such access must create and publicize appropriate policies and guidelines delineating responsibilities to ensure appropriate security.

6.1. Responsibilities for Fort Valley State University (Authorizing PODs) Fort Valley State University, when permitting PODs, should, at a minimum:

- Determine the types of devices and software versions that are permitted.
- Define the minimum level of access controls, which may include device registration.
- Enroll and unenroll PODs including management of the device partitioned, if needed, for USG business.
- Detail which non-USG PODs applications are supported to access nonpublic information resources.
- Specify the types of monitoring, data protection and safeguards for permitted PODs.
- Collaborate with Human Resources to disclose to employees the type of action taken on PODs by the organization when separating from the organization.
- Describe what organizational information, if any, is permitted on personal devices.
- Provide a disclaimer of liability for personal data loss.
- Notify users of PODs the disclosure requirements under the Georgia Open Records Act.
- *Reference:* USG ITHB (v2.9.9), Section 5.2.2 Mobile Workforce Requirements.

6.2. Responsibilities for Users of PODs Users of PODs should, at a minimum:

- Maintain personal device software by installing firmware, operating system and application updates promptly.
- Implement access controls, e.g., fingerprint, facial recognition, or PIN, to unlock and access the device.
- Safeguard USG account credentials and use multi-factor authentication to access enterprise applications from PODs.
- Use an approved password manager to converge passwords between devices.
- Use the organization-approved Virtual Private Network (VPN) service and the organization’s supported VPN client software.
- If possible, enable endpoint firewall and antivirus protection.
- Back up any locally stored USG data regularly to USG-approved storage systems.
- Do not use unauthorized third-party software or storage facilities for accessing USG information.
- Install security patches in a timely manner.
- Cooperate with USG cybersecurity and/or technology teams performing relevant investigations.
- Report USG data loss from personal devices, misuse, or violation of this standard promptly.
- Comply with applicable policies and laws when using personally owned devices.
- Reference: USG ITHB (v2.9.9), Section 5.2.2 Mobile Workforce Requirements.

7. Enforcement

Every user has an obligation to report suspected violations of this standard using the FVSU institution's incident reporting procedures or to the USG Shared Service Center. Violations of this policy may result in loss of FVSU system and network usage privileges, and/or disciplinary action (up to and including termination or expulsion) as outlined in applicable FVSU policies. Furthermore, any user engaging in unethical and/or inappropriate practices that violate USG standards is subject to disciplinary proceedings that may include suspension of system privileges, expulsion, termination and/or legal action as appropriate. If a user is suspected of violating USG standards or policy, any right to privacy may be superseded by USG's requirement to protect the integrity of IT resources, the rights of all users and state assets. The USG reserves the right to examine material stored on or is transmitted through IT resources to maintain appropriate standards of conduct and duty of care. If a user suspects that they are a victim of a violation of this policy, then the violation may be reported directly to the FVSU Cyber Security team by sending an email to ithelpdesk@fvsu.edu per the Incident Reporting procedures found in the Incident Response Plan.

8. Policy Terms

FVSU IT Resources: FVSU-owned computers, networks, devices, storage, applications, or other IT equipment. "FVSU owned" is defined as equipment purchased with either University funding (including sources such as Foundation funds etc.) or Sponsored Research funding (unless otherwise specified in the research agreement).

9. Policy Review and Updates

This policy shall be reviewed [annually/biannually, consistent with USG ITHB requirements] or as needed in response to significant changes in risk posture, technology, or relevant regulations and policies, including updates to the USG Information Technology Handbook.

If a user suspects that they are a victim of a violation of this policy, then the violation may be reported directly to the FVSU Cyber Security team by sending an email to ithelpdesk@fvsu.edu per the Incident Reporting procedures found in the Incident Response Plan.

Revision Record			
Date	Revised by	Version	Change Reference
6/2020	Ndidi Akuta	1.0	Initial Creation
6/22/2023	Ronald Smalling	1.0.1	Minor wording changes
7/10/2025	Ronald	2.0	Updated document to include: -Personally owned devices -More prohibited activities -Update terminology