FVSU (IT) Password Policy

1. **Overview / Purpose**

Passwords are one of the primary mechanisms that protect Fort Valley State University information systems and other resources from unauthorized use. Constructing secure passwords and ensuring proper password management are essential. Poor password management and construction can allow both the dissemination of information to undesirable parties and unauthorized access to university resources. Poorly chosen passwords are easily compromised. This document establishes the minimum standards for password creation and management used by Fort Valley State University's computing accounts, in alignment with the University System of Georgia (USG) Information Technology Handbook (ITHB) (v2.9.9). This policy also outlines enforcement for password policy violations.

2. **Scope**

This policy applies to all accounts on computing resources administered by Fort Valley State University, including but not limited to user accounts, maintenance accounts, and service accounts. This policy applies to all individuals (employees, faculty, staff, students, contractors, affiliates, and guests) who access, process, store, or transmit University information or access University IT resources.

3. **Policy Requirements**

3.1. Authentication Standard Fort Valley State University shall deploy cost-effective technical and procedural measures to establish user identification, implement authentication, and enforce access rights. All users and their activity on IT systems, products, or services should be uniquely identifiable. User access rights to all systems and data must be in line with defined and documented business needs and job requirements and must be attached to user identification.

- *Reference:* USG ITHB (v2.9.9), Section 5.12.1 Password Authentication Standard.

3.2. Multifactor Authentication (MFA) Securing information and information systems, products or services remains a core responsibility of Fort Valley State University. Alone, single sign-on authentication methods are at risk of compromise and no longer considered secure. To mitigate this risk, multifactor authentication (MFA) with separate factors must be implemented across Fort Valley State University. MFA shall be the standard for

accessing all USG or third-party managed resources by all Fort Valley State University employees, students, affiliates, and contractors.

- **Deployment Priorities:** Deployment may be implemented using a tiered approach beginning with:
    - **Tier I:** Systems, products, or services storing classified information (e.g., mission-critical systems, databases and warehouses, email and internet facing web servers, and portals).
    - **Tier II:** Systems, products, or services permitting privileged access (e.g., administrator roles), remote access, servers critical to supporting business function, and all single sign-on systems.
    - **Tier III:** All remaining systems, products, or services supporting the organization.
- **Personnel Affected:** Any faculty, staff, student, affiliate, and contractor that has access to any categorized USG or third-party managed resource.
- **Configuration Baselining:** Fort Valley State University shall securely configure MFA to limit legacy protocol bypass, direct local access, and protocols that weaken the safeguard's effectiveness. Additional settings to harden should be considered, such as push notification versus call or passcode, and time-out limits.
- **Exemption:** Instances where MFA is not an option (e.g., operational technology, legacy devices, research, medical devices, or sensors) must be inventoried, and the plan of action updated with mitigating controls if assessed risks are acceptable. All exceptions to safeguards standards must be submitted to the USG CISO for review and approval.
- *Reference:* USG ITHB (v2.9.9), Section 3.1.2 Multifactor Authentication.

3.3. Password Composition Requirements Access to all USG information systems, products, or services used to process, store, or transfer data with a security categorization of MODERATE or higher (as defined in USG ITHB, Section 5.6.2), shall require the use of a digital identity that contains strong passwords or other strong authentication mechanisms. Strong passwords shall be constructed with the following characteristics:

- Be at least fourteen (14) characters in length.
- Must contain characters from 2 types of characters:
    - English upper case (A-Z)
    - English lower case (a-z)
- Must not contain easily accessible or guessable personal information about the user or user's family, such as names, birthdays, pets' names, addresses, etc.
- Must be verified by Fort Valley State University against a list of passwords known to be commonly used, expected, or compromised; and if a known or compromised password is chosen, the user is prompted to select a new password.

- *Reference:* USG ITHB (v2.9.9), Section 5.12.1 Password Authentication Standard.

3.4. Password Protection Requirements A password shall be treated as confidential information and shall not be shared with anyone including, but not limited to, administrative assistants, system administrators, and helpdesk personnel. The non-sharing of credentials is an essential practice for ascribing system activity to users or processes.

- Users shall not write and store passwords in clear text anywhere in their office or publicly.
- Passwords shall not be stored in a file on any computer system, including smart devices, without encryption.
- Passwords shall not be inserted into email messages or other forms of electronic communication unless encrypted.
- Temporary or "first use" passwords (e.g., new accounts or guests) must be changed the first time the authorized user accesses the system and have a limited life of inactivity before being disabled.
- Default passwords shall be changed before going into production and no production passwords are to be used in test and development environments.
- If an account or password is suspected of being compromised, the incident must be reported in accordance with Fort Valley State University's incident response procedures.
- User accounts that have system or administrative privileges granted through group memberships or programs shall have a unique password from other accounts held by that user.
- User accounts that have been granted temporary administrative rights shall be configured to expire within 24 hours of receiving the rights.
- Password history must be enabled and configured to disallow the reuse of the same password for a set length of change cycles greater than four (4) times and with the same password that has been used in the past four (4) changes. Password change frequencies must be configured to limit repeated successive password changes.
- Account lockout, or other rate-limiting mechanisms, must be enabled to lock or disable the account after five (5) unsuccessful or failed login attempts. Temporary lockouts are permitted, provided the lockout period is longer than ten (10) minutes.
- *Reference:* USG ITHB (v2.9.9), Section 5.12.1 Password Authentication Standard.

3.5. Password Change Frequency

- If MFA is enabled, passwords must be changed every 365 days or at any time evidence suggests the current credentials are or were potentially compromised.

- If MFA is not enabled (e.g., legacy systems), passwords must be changed according to the following schedule:
    - Administrator-level passwords shall be changed every ninety (90) days.
    - User-level passwords shall be changed every year.
- Passwords used to safeguard regulated information must be changed in alignment with regulatory requirements (e.g., card holder data, research data, medical data, etc.).
- System-level (system-to-system or non-interactive services account) passwords shall be changed after a significant event (i.e., administrator departure, suspicion, or actual compromise event).
- *Reference:* USG ITHB (v2.9.9), Section 5.12.1 Password Authentication Standard.

3.6. Encrypted Authentication All networked devices are required to use encrypted authentication mechanisms in alignment with an organizational assessment of risk. Cryptographically sound encryption, or equally effective measures, is required for all personal, sensitive, or confidential information that is stored on portable electronic storage media and on mobile computing endpoints.

- *Reference:* USG ITHB (v2.9.9), Section 5.8.7 Encrypted Authentication.

4. Enforcement and Implementation The Chief Information Officer (CIO) of Fort Valley State University is responsible for enforcing this policy and is authorized to set specific password creation and management standards for FVSU's systems and accounts. Fort Valley State University is responsible for developing internal procedures to facilitate compliance with these USG security policies and standards.

5. Consequences and Sanctions Violations of this policy may incur the same types of disciplinary measures and consequences as violations of other Fort Valley State University policies, including progressive discipline up to and including termination of employment, or, in cases where students are involved, reporting of a Student Code of Conduct violation. Violations of this standard could result in serious cybersecurity incidents involving protected state, federal, or privacy data. Violators may be subject to disciplinary actions including termination and/or criminal prosecution. Systems and accounts that are found to be in violation of this policy may be removed from the FVSU network, disabled, etc. as appropriate until the systems or accounts can comply with this policy.

- *Reference:* USG ITHB (v2.9.9), Section 5.12.1 Password Authentication Standard (Enforcement).

Revision Record

Date	Revised by	Version	Change Reference
7/2020	Ndidi Akuta	1.0	Initial Creation
5/3/2021	Ndidi Akuta	1.0.1	Review
10/20/2022	Ronald Smalling	1.1	Minor wording changes
3/28/2023	Ronald Smalling	1.0.2	Added new logos, removed footer revision, and added table revision record
11/19/2023	Ronald Smalling	1.0.3	Cosmetic edits and wording changes
7/7/2025	Ronald Smalling	2.0	Overhaul