Virtual Private Network (VPN) Policy

I. Purpose

The purpose of this policy is to provide guidelines for remote access via Virtual Private Network (VPN) connections to the FVSU network that are in line with the University System of Georgia (USG) Information Technology Handbook (ITHB) section *5.2.2*.

II. Scope

This policy applies to all FVSU faculty, staff and approved third party utilizing VPN to access the FVSU network.

III. Policy

FVSU Virtual Private Network (VPN) service enables remote systems to connect to specified internal network resources directly. Approved VPN users must abide by all guidelines described in this policy. Users accessing VPN to access the network must recognize their responsibilities in line with FVSU's Acceptable Use Policy compliant with USG ITHB section *5.2.1*.

- Users must have a user account via an approved User Account Creation Form from HR.
    - **FVSU Employees** -User access to VPN is subject to an approval process and is to be initiated by their supervisor.
        - Supervisor is to provide the specific work use case for which VPN should be granted.
        - The form will then be sent to the employee where they will verify that they have read and understood FVSU's Acceptable Use Policy and VPN Access Request Policy.
        - The form proceeds to Information Security for its final approval. Once the form is fully approved FVSU's Systems Administration team will provide the access.

- **Auditors** – The VPN form is to be initiated by the FVSU point of contact for the audit.

    - The point of contact will need to upload/attach a copy of the Audit engagement letter and fill in the information requested about the auditor, including external contact details.
    - The form is then routed to the Chief Information Officer (CIO) and Information Security for approval. Once the form is fully approved FVSU's Systems Administration team will provide the access.

- **Vendor/Other third party** - The form is to be initiated by the Department Head who sponsoring said vendor/other third party.

    - A copy of the scope of work requiring access to VPN must be uploaded/attached by the Department Head and relevant external contact details provided as required by the form.
    - Once the form is fully approved FVSU's Systems Administration team will provide the access.

- Form initiators will only submit VPN Access Request Forms if the access is necessary and is appropriate for fulfillment of the employee's job responsibilities and consistent with FVSU's remote work policies.

- It is the responsibility of the employee with VPN privilege to ensure that unauthorized persons are not allowed access to their VPN session or credentials.

- Remote user-owned computers are subject to health checks of minimum safety standards when connecting to VPN.

- Remote user-owned computers connected to the VPN service are subject to the same policies that apply to on-campus access and should employ similar data security practices.

    - VPN User computers should have Anti-Virus software installed, an active firewall, the operating system and applications should have all updates applied.

    - Public wireless systems should only be used when absolutely necessary.

    - Public, shared use computers should NOT be used for VPN.

    - Computers accessing the VPN service should be dedicated to the VPN user.

    - VPN access to Banner or other systems which contain confidential data may be subject to additional approvals and restrictions.

    - RDP (Remote Desktop Protocol) access via VPN to employee workstations is

not allowed.

- Only VPN client applications authorized by the Fort Valley State Information Technology Department shall be used to connect to the VPN service.

- All VPN connections are logged and associated with the user.

- Use of VPN connections for collecting, downloading, or transferring confidential data, or to access resources for which the VPN user is not authorized, is prohibited. Per the FVSU Information Systems Security Policy, it is a violation to store confidential data on portable storage devices, including USB keys and portable disks, unless such data is encrypted.

- VPN access is good until April 30th of every year. On April 2nd, emails will be sent out to all VPN users requiring a new access form to be submitted. Failure to submit the access form by April 30th will result in your VPN access being removed.

- Remote computers connected to the VPN become an extension of the FVSU data network and are therefore subject to the same network use guidelines and policies extended to any other host on the network.

- VPN access requests or renewals can be made electronically by going to our forms page andclicking on the VPN Access Request Form.

- VPN access is restricted to FVSU managed devices. This means the device used to connect to FVSU's VPN must be an FVSU assigned computer provided by the Information Technology (I.T.) department. Devices that are not FVSU managed accessing the VPN will have their VPN session terminated. Minor exceptions exist for technical troubleshooting.

IV. Enforcement

This policy regulates the use of all VPN services to the FVSU network and users must comply with the Acceptable Use Policy and VPN Access Request Policy. VPN services will be terminated immediately if any suspicious activity is observed. Service will remain disabled until the issue has been identified and resolved. Any FVSU employee found to have intentionally violated the VPN Acceptable Use Policy will be subject to loss of VPN privileges. By choosing to use the FVSU VPN service, you hereby agree to all terms and conditions listed above. Further information is contained in the University's Information Security Policy, which may be accessed on the Office of Information Technology policies page, https://www.fvsu.edu/information-technology-policies/.

Revision Record			
Date	**Revised by**	**Version**	**Change Reference**
06/2020	Ndidi Akuta	1.0	Initial Creation
5/3/2021	Ndidi Akuta	1.0.1	Review
10/8/2022	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
4/7/2023	Ronald Smalling	1.0.3	Restrictions section was added to the policy
5//10/2025	Ronald Smalling	1.0.3	Annual Review
6/3/2025	Ronald Smalling	2.0	Policy Overhaul