

POLICY: REMOTE ACCESS POLICY

Type of Policy: Network Access **Last Revised:** June 2, 2019

Policy Owner: Information Services & Institutional Assessment

Policy Contact: Sharlene Harris

VP of Information Services & Institutional Assessment

sharris@uvi.edu

1.0 Purpose

The purpose of this policy is to define standards for connecting to the University of the Virgin Islands' (UVI) network from any host. These standards are designed to minimize the potential exposure to UVI from damages which may result from unauthorized use of UVI's resources. Damages include the loss of sensitive or university confidential data, intellectual property, damage to public image, damage to critical UVI internal systems, etc.

2.0 Scope

This policy applies to all UVI students, faculty, staff, contractors, vendors, and agents with a UVI-owned or personally-owned computer or workstation used to connect to the UVI network. This policy applies to remote access connections used to do work on behalf of UVI, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, ISDN, DSL, VPN, SSH, and cable modems, etc.

3.0 Policy

3.1 General

- 1. It is the responsibility of UVI students, faculty, staff, contractors, vendors and agents with remote access privileges to UVI's network to ensure that their remote access connection is given the same consideration as the user's on-site connection to UVI.
- 2. General access to the Internet for recreational use by immediate household members through the UVI Network on personal computers is prohibited. Please review UVI's Acceptable Use Policy for details of protecting information when accessing UVI's network via remote access methods.
- 3. For additional information regarding UVI's remote access connection options, including how to gain access, troubleshooting, etc., contact the Information & Technology Services (ITS) Helpdesk at extension 1466 or via email to helpdesk@uvi.edu.

3.2 Requirements

- 1. Secure remote access must be strictly controlled. Control will be enforced via one-time VPN or network password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase, see the Password Policy.
- 2. At no time should any UVI student, faculty, staff, contractor, vendor, or agent provide their VPN or network login or password to anyone.
- 3. UVI students, faculty, staff, contractors, vendors, and agents with remote access privileges must ensure that their UVI-owned or personal computer or workstation, which is remotely connected to



UVI's network, is not linked to any other network at the same time, except for personal networks that are under the complete control of the user.

- 4. UVI students, faculty, staff, contractors, vendors, and agents with remote access privileges to UVI's network must not use non-UVI email accounts (i.e., Hotmail, Yahoo, Gmail), or other external resources to conduct UVI business.
- 5. Reconfiguration of a home user's equipment for split-tunneling or dual-homing is not permitted at any time.
- 6. Non-standard hardware and security configurations needed for access to hardware must be approved by IS & IA network department.
- 7. All hosts that are connected to UVI internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers. Personal equipment that is used to connect to UVI's networks must meet the requirements of UVI-owned equipment for remote access.
- 8. Organizations or individuals who wish to implement non-standard Remote Access solutions to the UVI network must obtain prior approval from the VP of IS & IA.

4.0 Enforcement

Any student, faculty, staff, contractor, vendor or agent found to have violated this policy may be subject to disciplinary action, up to and including termination of access to the network or employment, as stated in the Accessible Use Policy.