



## **Hampton University Virtual Private Network (VPN) Acceptable Use Policy**

### **I. Objective**

The purpose of this policy is to provide guidelines for Remote Access IP Security (IPSEC) Virtual Private Network (VPN) connection to the Hampton University campus network.

### **II. Scope**

This policy applies to all Hampton University faculty, staff, employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPN to access the Hampton University network.

### **III. Policy**

1. Installation and use is permitted only on Hampton University owned computers. Installation or use on personally owned and other non-University owned computers is prohibited.
2. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to Hampton University internal networks.
3. VPN use is to be controlled using a username and password authentication. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
4. VPN gateways will be set up and managed by the Center for Information Technology/Networking department.
5. All computers connected to Hampton's internal networks via VPN must use the most up-to-date anti-virus software available at the CIT/Networking department. All computers must have all current service patches and security updates installed.
6. VPN users will be automatically disconnected from Hampton University's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
7. The VPN concentrator is limited to an absolute connection time of 24 hours
8. Only approved VPN clients may be used.
9. While Hampton's network administration desires to provide a reasonable level of privacy, users should be aware that for security and network maintenance purposes, authorized individuals within the CIT's networking services may monitor equipment, systems and network traffic at any time.
10. All Hampton University policies and procedures apply in addition to those stated above. For more information on the Hampton University Acceptable Use Policy please contact the CIT/Networking department at [networkops@hamptonu.edu](mailto:networkops@hamptonu.edu) or view at the [CIT website](#).

### **IV. Enforcement**

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.