Virtual Private Network (VPN) Policy

1.0 Purpose
The purpose of this policy is to provide guidelines for Remote Access IPSec or L2TP Virtual Private Network (VPN) connections to the Fuqua network.

2.0 Scope
This policy applies to all Fuqua faculty, employees, contractors, consultants, temporaries, and other workers (hereafter notes as “affiliates”) including all personnel affiliated with third parties utilizing VPNs to access the Fuqua network. This policy applies to implementations of VPN that are directed through the Duke University Office of Information Technology (OIT).

3.0 Policy
Approved Fuqua affiliates and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees. Further details may be found in the Remote Access Policy.

Additionally,

1. It is the responsibility of affiliates with VPN privileges to ensure that unauthorized users are not allowed access to Fuqua internal networks.
2. VPN use is to be controlled using Duke University credentials through a portal managed and maintained by OIT.
3. When actively connected to the Fuqua network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
4. Dual (split) tunneling is NOT permitted; only one network connection is allowed.
5. VPN gateways will be set up and managed by OIT.
6. All computers connected to Fuqua internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the University standard (http://oit.duke.edu/comp-print/software/index.php); this includes personal computers.
7. VPN users will be automatically disconnected from Fuqua'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.
8. The VPN concentrator is limited to an absolute connection time of 24 hours.
9. Users of computers that are not Fuqua-owned equipment must configure the equipment to comply with Fuqua's VPN and Network policies.
10. Only OIT-approved VPN clients may be used.
11. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of Fuqua's network, and as such are subject to the same rules and regulations that apply to Fuqua-owned equipment, i.e., their machines must be configured to comply with Fuqua's Security Policies.

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

5.0 Revision History

Date	Who made the revision	Change made
2012-01-23	Fuqua Infrastructure	Initial issue