Information Technology Security Plan
Remote Access Policy (10.14)

Responsible executive: CIO
Responsible office: ITS

Approval date: 7/01/2016
Effective date: 7/01/2016

Related policies: IT Security Plan, Appropriate Use Policy, Network Access Policy, Antivirus Policy

1.0 Policy Statement

It is the responsibility of users with remote access privileges to ensure their remote access connection from an un-trusted host is given the same consideration as a campus network connection. All remote computers connected to the university network via VPN must be up-to-date with the latest anti-virus software and system security patches.

2.0 Reason for Policy

The purpose of this policy is to establish guidelines for connecting to the university network from any remote un-trusted host.

3.0 Applicability

This policy applies to all employees, students, contractors and other university affiliates who have a remote un-trusted connection to the university network.

4.0 Terms and Definitions

Remote Access - Any access to university network through a non-university-controlled (un-trusted) network, device, or medium;

Virtual Private Network (VPN) – creates a secure connection (tunnel) to another network over the Internet, using authentication and encryption.

5.0 Policy

5.1 Remote Access Guidelines

Remote un-trusted connections to the university network must be made using supported VPN Web and desktop clients.

VPN services are configured and managed through Information Technology Services (ITS). VPN access may be requested by submitting a VPN request form to the Helpdesk. Contact the Helpdesk for VPN installation and connectivity assistance.

The VPN is a "user managed" service, i.e., the user is responsible for selecting an Internet Service Provider, coordinating the installation of required software and paying associated fees.

VPN use will be controlled using password authentication. It is the responsibility of users with VPN privileges to ensure that unauthorized users are not allowed access to the university network.

When actively connected to the university network, the VPN will force all traffic to and from the remote computer over the VPN tunnel; all other traffic will be dropped. Dual (split) tunneling is not permitted; only one network connection is allowed.

All remote computers connected to the university network via VPN must be up-to-date with the latest anti-virus software and system security patches.

By using VPN services with personal equipment, users must understand that their machines are an extension of the university network and are subject to the same policies that apply to SSU-owned equipment.