Telework Policy Security Supplement

Overview

In an effort to provide a secure, confidential, and reliable environment for those who are teleworking, SU has created this policy supplement outlining the steps the University takes and teleworkers should take to maintain a secure telework environment.

Telework Guidelines

When using a personal device the employee is responsible for ensuring the device meets the criteria below:

- No Personally Identifiable Information (PII) is allowed to be stored on personal computing devices
- Personal devices should be patched to the latest software available by the manufacturer
- Personal devices should be protected by security software which looks for threats on the device
- All connections into the SU network should be through the use of SU's provided VPN service

When using a SU provided device the employee is responsible for adhering to the same SU endpoint security standards as on campus. Note, from time to time SU may request the device be brought to campus for security updates.

Telework environment

- Steps should be taken to ensure other individuals cannot see your screen in your telework environment
- Care should be taken when accessing any networks not under your control

SU Controls

Control	Description
Remote Access	SU provided two forms of remote access • Always-On VPN - This VPN service is built into University Laptops and will automatically connect to University resources • On-Demand VPN - This VPN service can be used on personal devices and requires Multi-factor Authentication and in limited in scope to the University resources it can access
Software	University provided software can only be installed on University devices.

Definitions

Remote Access - Defined by accessing SU hosted resources which are not otherwise publicly available.