1. If personally owned computers, tablets or smartphones are going to be used for conducting WSU business, it should not be a shared device that is accessible by multiple people.
2. Operating system and application software should be up-to-date.
3. All security patches should be up to date. Software should be set to automatically update.
4. Anti-virus software should be installed with updated software and virus definitions. Software should be set to automatically update.
5. Endpoints should have Fireeye Endpoint Agent and Splunk Universal Forwarder software installed so endpoint logs can be monitored in ITS central logging server and monitoring server.
6. Endpoints used by employees for processing, storage, and transmission of any WSU data requires full disk encryption on endpoints and on all data storage devices.
7. Processing, storage, and transmission of Regulated and WSU Confidential data from a remote site requires a VPN to facilitate the remote connectivity WSU internal resources.
8. Processing, storage, and transmission of Public or WSU Internal data from the remote site to WSU internal resources should use SSL/TLS enabled applications.
9. Endpoints should have WSU data backed up to a storage location owned and maintained by a WSU IT department to ensure ongoing access and protection against loss of critical WSU data.
10. Endpoints that do not require wireless usage should have wireless capability disabled prior to deployment.
11. Endpoints should be registered & joined to a WSU Area, College, or departmental domain.
12. Host-based firewalls should be enabled and appropriately configured.

For questions please contact, WSU Information Technology Services.