Minimum Security Standards for EndPoints

End Point Security - University Owned

Standards	What to Do	Low Risk	Moderate Risk	High Risk
Inventory	All university end points must be tracked in the ITS inventory.	●	●	●
Configuration Management	All university end points must be centrally managed to provide for updates and security controls.	●	●	●
Patching	Apply critical security patches within seven days of publish, all other high and medium level patches within 30 days. Use a supported OS version.	●	●	●
Whole Disk Encryption	Devices must use university managed whole disk encryption to protect against data loss if lost or stolen.	●	●	●
Malware Protection	Install ITS approved and supported anti-virus solution and configurations.	●	●	●
Backups	Backup user data at least dail to university provided solution. Ensure backups are encrypted in transit and while stored.	●	●	●
Inventory	All university end points must be tracked in the ITS inventory.	●	●	●
Regulated Data Security Controls	Implement hardened ITS PC standard configuration on device.			●

End Point Security - Personally Owned Used for University Work

Standards	What to Do	Low Risk	Moderate Risk	High Risk
Patching	Apply critical security patches within seven days of publish, all other high and medium level patches within 30 days. Use a supported OS version.	●	●	N/A - Not Permitted
Whole Disk Encryption	Devices must use whole disk encryption to protect against data loss if lost or stolen.		●	
Malware Protection	Install ITS approved and supported anti-virus solution and configurations.	●	●	
Backups	Backup St. Thomas user data at least daily to university provided solution. Ensure backups are encrypted in transit and while stored.		●	
Inventory	All university end points must be tracked in the ITS inventory.			
Regulated Data Security Controls	Implement hardened ITS PC standard configuration on device.			