

Minimum Security Standards for End Points

EndPoint Security- University Owned

Standards	What to Do	Low Risk	Moderate Risk	High Risk
Inventory	All university endpoints must be tracked in the IIS inventory.	●	●	●
Configuration Management	All university endpoints 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 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 IIS approved and supported anti-virus solution and configurations.	●	●	●
Backups	Backup user data at least daily to university provided solution. Ensure backups are encrypted in transit and while stored.	●	●	●
Inventory	All university endpoints must be tracked in the IIS inventory.	●	●	●
Regulated Data Security Controls	Implement hardened IISFC standard configuration on device.			●

EndPoint 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 supported OS version.	●	●	N/A- Not Relevant
Whole Disk Encryption	Devices must use whole disk encryption to protect against data loss if lost or stolen.		●	
Malware Protection	Install IIS 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 endpoints must be tracked in the IIS inventory.			
Regulated Data Security Controls	Implement hardened IISFC standard configuration on device.			