

	All university endpoints must be tracked in the IIS inventory.	●	●	●
	All university endpoints must be centrally managed to provide for updates and security controls.	●	●	●
	Apply critical security patches within seven days of publish, all other high and medium level patches within 30 days. Use supported OS version.	●	●	●
	Devices must use university managed whole disk encryption to protect against data loss if lost or stolen.	●	●	●
	Install IIS approved and supported anti-virus solution and configurations.	●	●	●
	Backup user data at least daily to university provided solution. Ensure backups are encrypted in transit and while stored.	●	●	●
	All university endpoints must be tracked in the IIS inventory.	●	●	●
	Implement hardened IISFC standard configuration on device.			●

	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 Remed
	Devices must use whole disk encryption to protect against data loss if lost or stolen.		●	
	Install IIS approved and supported anti-virus solution and configurations.	●	●	
	Backup St. Thomas user data at least daily to university provided solution. Ensure backups are encrypted in transit and while stored.		●	
	All university endpoints must be tracked in the IIS inventory.			
	Implement hardened IISFC standard configuration on device.			