SDSU Baseline # Minimal EndPoint Security Baseline

Implements:	SDSU Standard # Security and Configuration of Information Systems

Minimal EndPoint[1] Security Baseline

The Information Technology Security Office provides this as the most current baseline configurations.

Security Baseline	Description	✓
Endpoint Management	All SDSU endpoints must be enrolled on Microsoft Intune for Windows or Jamf for macOS.	
Local Device Password	All SDSU Endpoints require the local accounts to follow the Default Domain Password Policy requirements for User Accounts, including password complexity, minimum length, and to be reset annually.	
Antivirus	All SDSU endpoints must have Microsoft Defender AntiVirus installed.	
Auto-Lock	To protect unauthorized access to the endpoint, an auto-lock must be configured. The default value is 15 minutes of inactive. Other values are possible, as needed by different use cases.	
Security Updates (OS)	All endpoints must apply OS security updates no longer than 30 days after release.	
Supported OS	All SDSU endpoints must be running vendor supported Operating Systems (OS).	
Security Updates (Apps)	All apps running on SDSU endpoints must apply patches and security updates.	
Host Based Firewall	All SDSU endpoints must have the host based firewall enabled.	
Encryption	All SDSU endpoints must have the hard drive encryption enabled.	

[1] An endpoint is defined as any laptop, desktop, or mobile device.