Fredonia Minimum Security Standards: Endpoints

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

Follow the minimum security standards in the table below to safeguard your endpoints. NOTE: All personally owned endpoints that are use to access (store or transmit) University data are required to adhere to these Minimum Security Standards.

STANDARDS	RECURRING TASK	WHAT TO DO ?	LOW RISK	MODERATE RISK	HIGH RISK
Patching		Apply security patches within seven days of publish. Use a supported OS version.			
Whole Disk Encryption Desktops		Enable FileVault2 for Mac, BitLocker for Windows. Install MDM on mobile devices.			
Whole Disk Encryption Mobile Devices		Enable FileVault2 for Mac, BitLocker for Windows. Install MDM on mobile devices.			
Malware Protection and Intrusion Prevention		Install antivirus (Symantec End Protection (SEP) recommended).			
Backups		Back up user data at least daily. Encrypt backup data in transit and at rest.			
Inventory		Review and update records quarterly. Maximum of one node per record.			
Configuration Management		TBD			
Regulated Data Security Controls		Implement PCI DSS, HIPAA, FISMA, or export controls as applicable.			
Two-factor Authentication		Require Duo two-factor authentication for interactive user and administrator logins.			
Security Training		Complete annual Secure the Human Training.			

Short URL to this page: https://answers.fredonia.edu/x/$action.getTinyUrl()

Related articles

- Fredonia Mail Data Loss Prevention Policy for Credit Card Numbers (CCN) and Social Security Numbers (SSN)
- Procurement Standards
- Can I use the Duo Security internationally?
- Do I need a smartphone to use Duo?
- If I choose to use my personal smartphone using the Duo Mobile app, what kind of information does Duo have access to?