Core Security Standards - Endpoints						
Title	**Recurring**	**What To Do**	**Low Risk**	**Moderate Risk**	**High Risk**	**Reference Link(s)**
Patching	Yes	**Keep all software (OS and application) up to date to the extent possible.** Critical updates/patches shall be applied within 5 days, normal patches within 30 days. Only use actively-supported Operating Systems and applications. Systems with unsupported or outdated OS and applications may not be directly connected to the campus network.	Yes	Yes	Yes	IT-08 Network Citizenship Policy IT Standard 05 - Computer Security Standard
Inventory	Yes	**Utilize campus, college, or unit inventory service/procedures to track all devices.**	Yes	Yes	Yes	UI Controller's Computer Inventory & Control Policy
Media Disposal	No	**All institutional data and licensed software must be reliably erased from all devices prior to transfer within the UI, and wiped before leaving University control.** All end-of-life data storage hardware, after being erased, but be transferred to UI Surplus. If data cannot be erased, the media must be destroyed. Research data must be approved by the OVPR before it can be transferred out of University control. UI Record data (Official and Convenience) must be destroyed in accordance with UI Records Management Policy	Yes	Yes	Yes	IT-21 Computer Data and Media Disposal Policy UI Surplus Homepage UI Routing Policy, Procedure UI Guidebook on Records Management
Whole Disk Encryption	No	**Whole disk encryption is required on all laptops and tablet computers, USB storage devices with Level III data, and for desktops in units that regularly handle Level III data.** Enable FileVault2 for Mac, BitLocker for Windows, BitLocker2Go for Windows USB devices, LUKS or similar software for Linux. Systems must be domain-attached and using device management to use whole-disk encryption.	Yes	Yes	Yes	IT-18 Information Security Framework IT-19 Institutional Data Access & Handling Policy IT Standard 05 - Computer Security Standard ITS - Encryption Help
Backups	Yes	**Institutional data should not be stored locally.** If there is a business requirement to store institutional data locally, data must be backed up in accordance with the UI Records Management Program System and data backups must exist to enable prompt recovery/restoration of service.	Yes	Yes	Yes	IT-17 Backup & Recovery Policy UI Operations Manual, Ch. 17 - Records Management ITS Storage Options Summary Chart
Incident Handling	Yes	**All suspected or confirmed security incidents must be immediately reported to the Security Office.** No actions, including but not limited to sensitive data scans (IdentityFinder), repairs, reimaging, copying data, or other actions, may be performed without prior direction from the Security Office.	Yes	Yes	Yes	IT-06 Security Incident Escalation Policy Report a Security Incident
Physical Protection	No	**All endpoints must be kept in a physically secure location when staff are not present.** Laptops and Tablets must be physically secured when not in use. Location must be protected by physical access controls such as key, or proximity cards.		Yes	Yes	IT-18 Information Security Framework Policy

Configuration Management	Yes	**Automated system change control management must be utilized for devices, such as UI Capser or MS-SCCM services.** CM process must monitor and control hardware and software configuration changes.		Yes	Yes	IT-18 Information Security Framework IT Standard - 05 Computer Security Standard ITS - Mac and iOS Management ITS - System Center Configuration Manager
Regulated Data Security Controls	No	**Implement additional requirements in accordance with applicable regulations.**			Yes	UI Information Security Plan IT Security - HIPAA General Information IT Security - PCI-DSS Compliance IT Security - FISMA Resouces Research Data Routing Policy Research Security Plan Template