Minimum Security Standards for IoT Devices

Internet of Things (IoT) Devices

Standards	What to Do	Low Risk	Moderate Risk	High Risk
Inventory	All university IoT devices must be tracked in the ITS inventory.	●	●	●
Network Isolation	IoT devices used to support university business or research should categorized and assigned on the network in a way that isolates them other campus services, and allow access to the internet only when absolutely necessary.	●	●	●
Patching	Based on National Vulnerability Database (NVD) ratings, apply critical severity security patches within 14 days of publish, high severity within 30 days, and all other security patches within 90 days. Use a supported OS version.	●	●	●
Vulnernability Management	Perform a quarterly vulnerability scan. Remediate critical level vulnerabilities within seven days of discovery and high level vulnerabilities within 90 days.	●	●	●
Credentials & Access Control	Review existing accounts and privileges quarterly. Enforce password complexity.	●	●	●
Centralized Logging	Security event logs must be forwarded to ITS Information Security remote log server.		●	●
Security, Privacy, and Legal Review	Request a Security, Privacy, and Legal review and implement recommendations prior to deployment.			●
Regulated Data Security Controls	Implement PCI DSS, HIPAA, or export controls as applicable.			●

Version 1.0 - Updated January 11, 2023