Minimum Security Standards for Applications

Applications

Standards	What to Do	Low Risk	Moderate Risk	High Risk
Risk Assessment	Application is put through ITS risk assessment process prior to aquistion. All identified risks must be accespted by the Data Owner(s). EDUCAUSE HECVAT or HECVAT Lite are preferred assessement tools.	●	●	●
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.	●	●	●
Vulnerability Management	Perform a quarterly vulnerability scan. Remediate critical level vulnerabilities within seven days of discovery and high level vulnerabilities within 90 days.	●	●	●
Inventory	Application is added to the ITS Application Inventory Database.	●	●	●
Firewall	Enable host-based firewall in default deny mode and permit the minimum necessary services.	●	●	●
Credentials and Access Control	Review existing accounts and privileges quarterly. Enforce password complexity. Logins with UST domain accounts whenever possible using SSO.	●	●	●
Multifactor Authentication	Require multifactor authentication for all interactive user and administrator logins.		●	●
Centralized Logging	Security event logs must be forwarded to ITS Information Security remote log server.		●	●
Developer/Application Owner Training	Developers and administrators must complete information security related training per guidelines for specfic data and compliance areas covered.		●	●
Secure Software Development	Include security as a design requirement. Review all code and correct identified security flaws prior to deployment. Use of static code analysis tools recommended.		●	●
Security, Privacy, and Legal Review	Request a Security, Privacy, and Legal review and implement recommendations prior to deployment.		●	●
Formal Security Risk Assessement Required	Complete a HECVAT or HECVAT Lite risk assessment, and address concerns upon acquisition and at least every 3 years once in production.		●	●
Dedicated Admin Workstation	Access administrative accounts and systems only via a certified Priviledge Access Workstation.			●
Regulated Data Security Controls	Implement PCI DSS, HIPAA, or export controls as applicable.			●

Version 1.0 - Updated January 11, 2023