Minimum Security Standards for Applications

Software as a Service (SaaS) Solutions

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.	●	●	●
Inventory	Application is added to the ITS Application Inventory Database.	●	●	●
Credential and Key Management	If possible, Integrate with Stanford's SSO services, preferably SAML. Review administrative accounts and privileges quarterly. Adhere to the Stanford password complexity rules if not integrated with a Stanford SSO service. API keys: Minimize their generation. Grant minimum necessary privileges. Rotate at least annually. Do not hardcode. Do not shre credentials	●	●	●
Encryption	Must use transport layer encryption TLS 1.2 or higher. Must use encryption of data at rest (if available)	●	●	●
Multifactor Authentication	Require multifactor authentication for all interactive user and administrator logins. Use St. Thomas SSO and MFA if offered by solution.		●	●
Centralized Logging	Enable any available application logging that would assist in a forensic investigation in the event of a compromise. Seek vendor or ISO guidance as needed. Contractually ensure that the provider can export logs at the request of Stanford within five days.		●	●
Secure Admin Workstation	Administration consoles should only be accessed through a Privileged Access Workstation (PAW) when logging in with an administrative account. Administrative accounts are defined as: Accounts with the ability to make unrestricted, potentially adverse, or system-wide changes. Accounts with the ability to override or change security controls.		●	●
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