Minimum Viable Secure Product

Drexel University Information Security Office has developed a security checklist for third-party software and vendors. All third-party service providers and cloud-based vendors handling (store, process, or transmit) sensitive or confidential institutional data must have the following security controls to meet Drexel requirements for a minimum viable secure product (MVSP).

1. Business Controls	
Control	**Description**
Security Office and Program	A dedicated information security office and program for managing information security risk and ensuring compliance with industry standard security frameworks, and applicable regulations and standards.
Risk Management	A risk assessment process to identify and manage risks that could affect company's security posture and ability to provide reliable services to its customers.
Privacy Policy	A publicly posted Privacy Policy or notice to the public, users, or customers, describing how you protect the security and privacy of data.
Compliance	Comply with all industry standards, local laws, and regulations in jurisdictions, where applicable.
2. Authentication Controls	
Control	**Description**
Single Sign On	Support for single-sign-on (SSO) standards for user and administrator authentication using modern standards. Example: SAML2 and Shibboleth.
Password Policy	Maintain strong password policy including minimum length, complexity, lockout, expiration, and history. Meet university password requirements as listed below https://drexel.edu/it/help/a-z/password-self-service/.
Multifactor Authentication	If SSO is not supported, application and/or user frontend portal must support multifactor authentication (MFA)
Password Storage	User passwords must not be stored in plaintext and no passwords should be hard coded into the system or application.
Logging	All user actions including login, logout, actions performed, and source IP address must be logged and available to the institution.
3. Application Controls	
Control	**Description**
Firewall and Monitoring	The application and the institutional data should be protected by stateful packet inspection (SPI) firewall. There should be documented procedures for traffic and intrusion monitoring internally or by a third-party service.
Access Control	Support for role-based access control (RBAC), attribution-based access control (ABAC) or policy-based access control (PBAC) for users and administrators.
Web Application Firewall (WAF)	The application and the institutional data should be protected by web application firewall (WAF) to protect against common web vulnerabilities.
4. Data Controls	
Control	**Description**
Encryption	All institutional data must be encrypted in transit and at rest using strong encryption standards approved by The National Institute of Standards and Technology (NIST).

Infrastructure	All institutional data must be logically and/or physically separated from other institutions.
Backup	The application must meet backup frequency and interval requirements as set forth by the university department.
Datacenter	All institutional data should reside in datacenters located in the Institution's Data Zone, that is, United States. No data should be physically or electronically transported into a data zone that is not authorized by the institution.
5. Operational Controls	
Control	**Description**
Security Control Systems	Security control systems may include firewalls, IDS/IPS, next gen persistent threat (NGPT) monitoring, file integrity monitoring (FIM), antimalware, physical access controls, logical access controls, audit logging mechanisms, and network segmentation controls.
Secure Development	Developers must abide by security by design, privacy by design and follow FTC guidelines listed - https://www.ftc.gov/business-guidance/resources/app-developers-start-security.
Incident Handling	Incident handling protocols for the team and employees to follow to fix the security breach as soon as possible. Notify institution about the security incident/breach within a reasonable timeframe.
Vulnerability Scanning	Application and underlying systems must be scanned externally for vulnerabilities. Penetration test of the infrastructure must be performed at least annually.
Patching	All critical and high severity vulnerabilities must be patched based on NIST's National Vulnerability Database severity ratings.
6. Administrative Controls	
Control	**Description**
Business Continuity Plan (BCP)	A formal Business Continuity Plan which includes processes to address all mission-critical business processes.
Change Management	A formal change management process to ensure that all changes to systems, networks, and processes are appropriately reviewed and approved.
Disaster Recovery Plan (DRP)	A formal Disaster Recovery Plan which includes processes to ensure that the critical business processes will continue to operate if there is a failure of one or more information processing or telecommunication resources.
Security Policies	Documented and written policies, guidelines, and procedures for safe handling and protection of data.
Security Training	An information security awareness program and security awareness training mandatory for all employees. Role-specific security training for personnel that is relevant to their business function.
Background Checks	Documented process for background screenings or background checks for all employees with access to institutional data.

Version	Date	Comments
1.0	5/6/2022	Initial Release (Approved by Information Security Office)