Third-Party Vendor Data Security & Privacy Review

Chief Information Security Officer

Information and Technology Services

Date: December 17, 2025

Version: 1.0

Contact: itsecurity@memphis.edu

Third-Party Vendor Data Security & Privacy Review — Template

Instructions

Use this template to perform intake, risk tiering, documentation review, and ongoing monitoring of third-party vendors that process, store, transmit, or access institutional data. Send the questionnaire section to the vendor and attach their responses, HECVAT, and supporting artifacts (SOC 2, ISO 27001, PCI AOC, pen test summaries, …).

A. Intake & Scoping

Requesting Unit:

Business Purpose / Use Case:

Data Types & Classification:

System Integrations:

Hosting Model:

Availability Needs:

Prior Reviews/Approved Solutions:

B. Inherent Risk & Tiering

Risk Tier (high, medium, low):

C. Requested Documentation (attach as appendix)

☐ Completed HECVAT (current version)

☐ SOC 2 Type II report (or ISO/IEC 27001 certificate)

☐ PCI DSS AOC/SAQ + ASV scans/pen test summary (if applicable)

☐ Recent external vulnerability scan & remediation status

☐ Data flow diagram and architecture overview

Vendor Security & Privacy Questionnaire (HECVAT-aligned)

(This is not required if you have already completed the current version of the HECVAT.)

SECTION 1 — ORGANIZATION & SCOPE

- Service description, data types handled, and system boundaries (attach data flow diagram).
- Hosting model (SaaS/PaaS/IaaS/On-Prem), primary/backup data centers, and data residency.
- Subcontractors/third parties with access to our data; controls and oversight mechanisms.

Vendor Response:

SECTION 2 — GOVERNANCE, RISK & COMPLIANCE

- Current certifications/attestations (SOC 2 Type II, ISO/IEC 27001, PCI AOC/SAQ, …).
- Risk management program (assessment cadence, treatment), policy framework, executive ownership.
- Compliance evidence for FERPA, GLBA, HIPAA, PCI DSS, GDPR/CCPA (as applicable).

Vendor Response:

SECTION 3 — PRIVACY & DATA PROTECTION

• Privacy policy, data minimization/retention schedule, and lawful bases for processing.

• Consent/notice mechanisms; data subject rights handling (access, correction, deletion).

• De-identification/pseudonymization; analytics/testing environment controls.

Vendor Response:

SECTION 4 — SECURITY ARCHITECTURE & CONTROLS

• Encryption at rest/in transit (algorithms, key management, rotation).

• Identity & Access: SSO (SAML/OIDC), MFA, RBAC/ABAC, PAM, session controls.

• Secure SDLC: code reviews, dependency scanning, vulnerability management, change control.

• Provide last 12 months of external vulnerability scans, pen test executive summary, and remediation status.

Vendor Response:

SECTION 5 — LOGGING, MONITORING & INCIDENT RESPONSE

- Logging (events captured, retention, access), SIEM integration, anomaly detection.
- Incident response plan, breach notification commitments (timeframes), forensics approach, communications.
- Security/privacy incidents in past 24 months and corrective actions.

Vendor Response:

SECTION 6 — BUSINESS CONTINUITY & RESILIENCE

- Backup strategy (frequency, encryption, immutability), RPO/RTO, DR testing frequency/results.
- Capacity management, availability SLAs, single points of failure mitigations.

Vendor Response:

SECTION 7 — DATA INTEGRATIONS & INTERFACES

- Integrations/APIs (protocols, auth methods, scopes), webhooks, import/export formats, secure transfer.

- Segregation/isolation controls for multi-tenant environments.

Vendor Response:

SECTION 8 — ACCESSIBILITY & USABILITY

- Accessibility conformance report (VPAT/ACR) and accommodations for assistive technologies.

- UI/UX privacy notices and dark-pattern avoidance.

Vendor Response:

SECTION 9 — AI USE & MODEL GOVERNANCE (if applicable)

- AI/ML use: models (internal/third party), training data sources, privacy safeguards, leakage protections.
- Prompting/inputs handling, fine-tuning retention, opt-out mechanisms for institutional data.
- Bias testing, explainability, human-in-the-loop, model change management.

Vendor Response:

SECTION 10 — CONTRACTUAL & OPERATIONAL COMMITMENTS

- Acceptance of institutional Data Security Agreement (DSA) clauses.
- Insurance coverage (cyber liability); name institution as additional insured where applicable.
- Offboarding procedures (data return formats, deletion timelines, destruction certificates).

Vendor Response:

SECTION 11 — ATTESTATIONS

- Executive attestation of accuracy/completeness and agreement to annual reassessment or upon material change.

Vendor Response: