Information Technology Services Security Questionnaire

Vendor Software Security and Compliance Assessment

Purpose:

This questionnaire is designed to assess the security, privacy, and compliance posture of third-party vendors seeking to provide software solutions to Arkansas State University (A-State). The A-State IT Security team and CIO will review the responses to ensure that proposed solutions meet the university's security requirements and adhere to industry best practices.

Please complete all sections of this questionnaire. Incomplete responses may delay or disqualify the approval process.

A Higher Education Cloud Vendor Assessment Tool (HECVAT) may be submitted in lieu of this security questionnaire.

Instructions:

- Submit the completed questionnaire, along with attachments and supporting documentation, via email to security@astate.edu.
- For questions that do not apply to your solution, please mark them as N/A and provide justification if necessary.

---

1. General Solution Overview

1.1. Solution Name and Description:

Provide the name and a brief description of the solution or service being offered.

_____

1.2. Solution Delivery Model:

Is the solution hosted on-premises, in the cloud, or hybrid?

☐On-Premises

☐Cloud

☐Hybrid

- If cloud-based, please indicate the hosting provider.

_____

1.3. Data Sensitivity:

Does your solution store, process, or transmit any of the following types of sensitive data? Please check any that apply:

☐Personally Identifiable Information (PII)

☐Protected Health Information (PHI)

☐FERPA-regulated Data

☐Financial Aid/Controlled Unclassified Information (CUI)

☐Payment Card Information (PCI)

☐HIPAA/HITECH-regulated Data

☐Financial Data

(*If none apply, skip to Section 6)*

Please detail the types of data of any choices selected above (e.g., if PII is checked, specify what that data is, such as student names, addresses, SSN). Provide specifics for any selected items.

_____

1.4. Third-Party Dependencies:

Does the solution rely on third-party services or subcontractors for any functionality (e.g., hosting, data processing, support)?

☐Yes

☐No

- If YES, list all third-party providers and describe their role.

_____

2. Data Security and Privacy

2.1. Data Encryption:

Describe the encryption methods used to protect data *in transit* and *at rest*. Specify the encryption standards used (e.g., AES-256, TLS 1.2+).

2.2. Data Ownership and Control:

Confirm that Arkansas State University retains full ownership of all its data. How is this ownership enforced and what measures ensure the university has full control over its data?

2.3. Access Controls and Privileged Access Management:

Who within your organization has access to A-State's data? What processes are in place for managing access control, ensuring role-based access, and maintaining separation of duties?

2.4. Data Classification and Segregation:

Describe how you classify and segregate A-State's data from other customers or internal systems. Include information on multi-tenant environments if applicable.

2.5. Data Retention and Disposal:

What is your data retention policy? Describe the process for securely deleting or returning data at the end of the contract. Include timeframes and formats for data return.

2.6. Breach Notification:

Describe your breach notification protocol.

- How would your organization handle data breaches, what would the timeframe be for notification from discovery and who would be the point of contact within your organization?

3. Compliance and Certifications

3.1. Compliance with Industry Standards:

List the security frameworks and standards with which your solution complies (e.g., NIST, CIS Controls, HIPAA/HITECH, FERPA, PCI-DSS).

3.2. Independent Security Audits:

Do you undergo regular third-party security audits (e.g., SOC 2, ISO 27001)?

☐Yes

☐No

- If YES, how often are these audits conducted and how are findings remediated?

3.3. Service Level Agreement (SLA):

Attach your SLA. Does it include specific provisions for data security, availability and breach notification? Specify remedies for failure to meet SLA terms.

3.4. Vulnerability Management and Penetration Testing:

Do you conduct regular vulnerability assessments and penetration testing on the system?

☐Yes

☐No

- If YES, provide the frequency.

---

4. Business Continuity and Disaster Recovery

4.1. Business Continuity Plan (BCP):

Do you have a BCP in place? Provide a summary of your plan, including recovery time objectives and recovery point objectives. How frequently is this plan tested?

4.2. Disaster Recovery Plan:

Describe your Disaster Recovery Plan, particularly for systems handling A-State's data. What is your recovery strategy in the event of a data loss event or system failure?

4.3. Backup and Redundancy:

How often is data backed up? Do you maintain redundancy mechanisms to ensure high availability and minimal data loss?

---

5. Operational Security

5.1. Security Logging and Monitoring:

What types of security-related logs do you maintain and how long are they retained?

5.2. Incident Response:

Describe your incident response plan, specifically addressing how security incidents involving A-State's data are managed. Include details on response time objectives, communication protocols and any escalation procedures.

5.3. Employee Security Screening:

What measures are in place to ensure that employees with access to sensitive A-State data are properly vetted? Additionally, how do you implement separation of duties and enforce the principle of least privilege for staff?

5.4. Support and Maintenance:

What are your technical support response times? Specify time zones and hours of operation.

- How will Arkansas State University be notified of upgrades, patches, or other system changes? Provide lead times for such notifications.

---

6. Legal and Regulatory Compliance

6.1. Liability for Data Breach:

What liability coverage is provided in the event of a data breach affecting A-State?

- Specify coverage details (e.g., per incident, per record, or per person affected).

6.2. E-Discovery and Legal Requests:

How will you handle legal requests for data (e.g., e-discovery, subpoenas)? What is your notification process to Arkansas State University for such requests?

6.3. Credit Card Processing (PCI-DSS):

If your system processes credit card payments, provide or attach evidence of PCI-DSS compliance. Include or attach any third-party certifications.

6.4. Gramm-Leach-Bliley Act (GLBA) Compliance

Does your solution process, store, or transmit any financial information that falls under the Gramm-Leach-Bliley Act (GLBA)?

☐Yes

☐No

7. Additional Information

7.1. End-User Compliance Considerations:

If the software application is to be used by faculty, staff, and/or students, a Voluntary Product Accessibility Template (VPAT) MUST be on file with both the Procurement office and ITS.

Signature

By Signing below, each party acknowledges that they have read and understood this questionnaire and agree that the answers provided are accurate and acceptable. Each party has signed as designated by its authorized representative.

Arkansas State University — Jonesboro
Information Technology Services

Name: _____

Title: _____

Date: _____

X _____

A-State Representative Signature

Mailing Address

PO BOX 1140
State University, AR 72467

Company: _____

Product: _____

Dept: _____

Name: _____

Title: _____

Date: _____

X _____

Vendor Representative Signature

Mailing Address

Street: _____

City: _____

State/ZIP: _____

Billing Contact (If Different From Above)

Street: _____

City: _____

State/ZIP: _____