# IT Data Security, System Performance and Service Reliability Questionnaire

Answers to the following questions will be reviewed and approved by the Arkansas State University IT Security team and the CIO to assure that providers system performance and service reliability meet A-State needs. Please send written response and attachments via email to Timothy Cureton tcureton@astate.edu – CISO, and to Henry Torres htorres@astate.edu – CIO.

1. Is this solution hosted or cloud-based?
2. Is this solution used to house or process restricted (PII, HEPA, FERPA, PCI) data?

   _____
   If questions one and two are NO, there is no need to completed the remainder of the questions.
   _____

3. How will we receive advance notice of upgrades or system changes?
4. Are there and/or will there be any subcontractors and business partners involved with our application and data?    If so, list who these entities are and verify that they are bonded?  Do you conduct security background checks on them?
5. What is your business continuity and disaster recovery plan?   Provide details.
6. Do you perform independent audits of your data center? How often? Provide details?
7. Is the storage of our data on your system encrypted in transit and at rest and by what means?
8. What is your specific Service Level Agreement (SLA) and does it include security of our data?
9. What type of security audit logs are kept?  What reporting do you provide for our periodic audit review?
10. We classify our data that will be stored on your system as PII and PHI.  How do you classify our data and what means of security do you use for this classification?
11. What are your proprietary and non-proprietary security processes?
12. Do you own, operate, and service the hardware and network infrastructure provisioned to run the system that you are providing as a service?
13. Do you conduct security background checks for the employees working and supporting our system?  Do they have appropriate separation of duties for control purposes?  Please provide details?
14. We reserve the right to request the removal of your employee, staff, subcontractor, from our account – how will you handle this if it is necessary?
15. What is the timeframe and the format that our data will be returned to us if the contract terminates?
16. We require immediate notification within 24 hours of any e-discovery or other legal requests related to our system and our data.  If this occurs, how will we be notified and by whom?
17. What is your liability coverage for any data breach that might occur?   Is it per incident, per record, or per person?  What is your notification plan to all impacted users for any data breach occurrence?
18. We require immediate disclosure and notification within 24 hours of any unauthorized data theft or breach as required by the State of Arkansas.  How will you manage this and are you prepared to do this if it occurs?
19. What means do you provide for us to import and export data freely at any time?
20. We require the use of U.S. data centers, can you provide assurance that this is being provided?
21. What are your tech support response times and on what time zone?
22. What access will you have to our data and who from your company will have this ability?
23. What means do you provide as reassurance that we own the data within your systems and services?
24. If you will process credit cards with data we provide, and/or if you sub-contract this process to a third party entity, please provide a copy of your current PCI and/or relevant certificate of compliance.

25. Please provide the statement of work and data flow of your application along with a description of how your application operates.
26. If the software application will be used by faculty, staff, and/or students, then we must have a Voluntary Product Accessibility Template (VPAT) on file in the office of Procurement and also in ITS.

**SIGNATURES**

In acknowledgement that the parties below have read and understood this Questionnaire and agree that the answers provided are true and acceptable, each party has caused the Questionnaire to be signed and transferred by its respective authorized representative.

**Arkansas State University – Jonesboro**
**Information and Technology Services**

By: _____
Name: _____
Title: _____
Date: _____

**Mailing Address:**
PO Box 1140
State University, AR 72467

**Company**:
_____

**Product:**
_____

Dept._____
By: _____
Name: _____
Title: _____
Date: _____

**Mailing Address**:
Street: _____
City:   _____
State/ZIP: _____

**Billing Contact (If different from above):**
Street: _____
City:   _____
State/ZIP: _____

9/24/2018