Accessibility Questionnaire

The following questions are used to determine if an application meets technical standards necessary for accommodating individuals with disabilities including auditory, cognitive, neurological, physical, speech, and visual disabilities. Please answer the following questions where applicable.

1. Do you have a Voluntary Product Accessibility Template (VPAT) completed? If so, please include a copy with your response to this questionnaire.

2. What has your company done to evaluate the accessibility of your product in accordance with either Section 508 of the Rehabilitation Act or WCAG 2.0 accessibility guidelines?

3. Do you know of any problems or have you received any complaints regarding the accessibility of your product? Please explain.

4. Has your product been evaluated using screen reading or voice recognition technology?

5. Can your product be navigated by using the keyboard only?

6. If accessibility for users with disabilities has not been implemented, when is your company planning to incorporate accessibility into the product?

7. If our users should encounter issues with accessibility, to what extent are you willing to work with the University to improve your product's accessibility?

8. If you know of organizations using your product for whom accessibility was also a priority, please provide contact information.

Data Security Vendor Questionnaire

The following questions are used to help protect sensitive data that is shared between Auburn University and entities whose servers and applications utilize the data. Please answer the following questions where applicable; Mark non-applicable questions as N/A.

Representative Information: This section pertains to the person completing questionnaire. Please provide complete information so we can contact you for additional questions or clarifications if the need arises.

- Name
- Title
- Phone number
- Email address

General Information

- Company Name
- Company Address
- Company Website

Product or Service Information

1. Provide a brief description of your product or service.
2. Does this product or service capture and/or retain any of the following? (Indicate all that apply)
   a. Names
   b. Addresses
   c. Date of Birth
   d. Social Security Number
   e. Health Information
   f. Department of Defense Information
   g. Banking Information
   h. Credit or Debit Card Information
   i. Grades
3. Will your employees have access to Auburn University data? (Indicate all that apply)
   a. Human Resource
   b. Student Information
   c. Financial Records
4. Describe your web application security standards? Do you meet OWASP standards?

Application Support and Training

5. Describe your on-line help.
6. What is the process for handling password resets?
7. What is the procedure for handling customer requests for application modifications?
8. How often is the application modified and how do you notify your customers of an upcoming modification?
9. Does your application allow the customer to export application data into a standard format such as Excel?

Availability
10. What is your application/service available uptime? Scheduled maintenance window?
11. How do you scale your system during peak usage?

Data Protection
12. How do you separate AUM's data from other customers' data?
13. Are there any indemnity provisions (in the contract) that protect AUM from any liability arising from a loss sensitive information?
14. Describe your data-at-rest and data-in-motion protection.
15. What encryption methods are used for data-at-rest and data-in-motion?
16. What kind of authentication and access control procedures are in place?
17. How do we send our data to you?
18. What methods do you use to transfer data from one place to another?
19. Do you currently utilized Multi-factor authentication to access Servers, website, user logins? If no, do you have plans to move to MFA?
20. What are your data loss prevention capabilities?
21. Is it possible for any third party (your service providers) to access data, and if so, how?
22. Is your secure gateway environment certified by an authoritative third party, and if so, who?
23. Has a security audit been performed to any of the following standards: PCI-DSS, CIS Security Benchmarks, ISO 27001/2, NIST 800-12, AICPA SOC 2 - Type II, or other (please name)? What are the results of the audit? Please included a copy of the external attestation.
24. Is sensitive data (e.g., payment card number, SSN) masked/encrypted such that only authorized individuals have access to the data?
25. Do you have plans to move away from SSL v2/v3 to TLS v1.1 or later? If so, when?

Vulnerability Management
26. Do you perform penetration testing? Has an external firm performed penetration testing?
27. Describe your virus detection methods and software.
28. How often do you scan for vulnerabilities on your network?
29. How often do you scan for vulnerabilities within your web applications?
30. How do you protect against outside threats?

Identity Management
31. How do you secure user IDs and access credentials?
32. Do you support SSO and if so, which standards?

Physical and Personnel Security
33. Do you restrict and monitor your employee access to data 24x7? 34. Do you perform background checks on all relevant personnel?
35. What were the findings of your most recent security audit? Date performed?
36. Do you use your own computing environment (including back-up and storage capacity)?
37. Do you use any 3rd party repository for file transfer, file storage or file sharing? (Ex. Dropbox, Office 365, Google Drive)?

Incident Response

38. What detection methods do you have to determine if the data has been breached by an outside source? (Intrusion Detection Systems)
39. What is your procedure for handling a data breach and how will AUM be notified?

Business Continuity (BC) and Disaster Recovery (DR)
40. What is your recovery point objective (RPO)?
41. What is your recovery time objective (RTO)?
42. Are your infrastructure components fully redundant?

End-of-service Support
43. Will data be packaged and delivered back to AUM at the end of service? If so, in what format and how soon will it be delivered?
44. How will you ensure that any AUM data will be destroyed completely from your network at the end of service?