Shelby County Schools Information Technology
Vendor Assessment Questionnaire

Company Name: _____ Company Website: _____
Responder Name: _____ Date of Response: _____

Service Overview

1. Name of application or service being provided:

2. Description of application or service:

3. What technology languages/platforms/stacks/components are utilized in the scope of the application? (Azure? MySQL? Ruby on Rails? Go? JavaScript?):

4. Is your service run from your own (a) data center, (b) the cloud, or (c) deployed-on premise only Data Center Location(s) (relative to services provided)?

5. Which cloud providers do you rely on?

6. Have you researched your cloud providers best security practices?

7. Which data centers/countries/geographies are you deployed in?

Please attach the following documents for review (if existing)

1. Most recent Application Code Review or Penetration Testing Reports (carried out by independent third party)
2. Information Security Policies and Procedures
3. Data Flow Diagram
4. Any other Documents supporting your responses in this questionnaire (Please provide a description for each document).
5. PCI, SOC2 type II or ISO27001 certification reports
6. Other Independent Audit report (please provide details)

Data Protection & Access Control

1. Please describe the company/user data you require to provide your service: personal information, financial data, confidential/sensitive data.

2. How do you encrypt customer data? Please submit all relevant documentation

3. Describe how your organization decides who does and does not have access to sensitive data

4. Please describe your general rules management in relation to role provisioning, deprovisioning, and recertification.

5. Which groups of staff (individual contractors and full-time) have access to personal and sensitive data handed to you?

6. Describe the circumstances in which customer data is allowed to leave your environment?

7. Describe the data retrieval process at termination of contract or engagement and include data format options.

Shelby County Schools Information Technology
Vendor Assessment Questionnaire

Authentication

Internal Use

1. Do you have an internal password policy?
2. Do you have complexity or length requirements for passwords?
3. How are passwords hashed?
4. Is MFA required for employees/contractors to log in to production systems?
5. Do internal applications leverage SSO for authentication?

Third Party Data Processing

1. Which processors (vendors) access your customer's information?
2. Do these processors (vendors) contractually comply with your security standards for data processing?
3. How do you regularly audit your critical vendors?

Policies and Procedures

1. Do you have an Information security risk management program (InfoSec RMP)?
2. Do you have management support or a security management forum to evaluate and take action on security risks?
3. Do you have a dedicated information security team? If so, what is the composition and reporting structure?
4. Do your information security and privacy policies align with industry standards (ISO-27001, NIST Cyber Security Framework, ISO-22307, CoBIT, etc.)?
5. Do you have a policy exception process?
6. Are all employment candidates, contractors and involved third parties subject to background verification (as allowed by local laws, regulations, ethics and contractual constraints)?
7. Are all personnel required to sign Confidentiality Agreements to protect customer information, as a condition of employment?
8. Are documented procedures followed to govern change in employment and/or termination including timely revocation of access and return of assets?
9. Do you have a communication policy that notifies the customer of changes in application or service security changes? If so, please explain or attach.

Proactive/Reactive Security

Shelby County Schools Information Technology
Vendor Assessment Questionnaire

1. How is your network security testing performed? Internal, third parties or both? If so, what is the cadence? Explain your methodology

2. How is your application security testing performed? Internal, third parties or both? If so, what is the cadence? Explain your methodology
3. Please summarize or attach your network vulnerability management processes and procedures?

4. What is your timeframe for patching critical vulnerabilities?

5. What tools do you use for vulnerability management?

6. What tools do you use for application vulnerability management?

7. How do you evaluate patches and updates for your infrastructure?

8. Do you publish a path for responsible disclosure of security vulnerabilities (ie security@ or /security)?

9. If applicable, are all endpoint laptops that connect directly to production networks centrally managed?

10. Describe standard employee issued device security configuration/features (ie AV, encryption, antimalware, etc).

11. Does sensitive or private data ever reside on endpoint devices? How is this policy enforced?

12. How do you limit data exfiltration from production endpoint devices?

13. What systems do you have in place that mitigate classes of web application vulnerabilities? (ie WAF, proxies, etc)

14. Do you have breach detection systems and/or anomaly detection with alerting?

15. Are changes to the production environment reviewed by at least two engineers/operations staff?

16. Are all security events (authentication events, SSH session commands, privilege elevations) in production logged?

17. Is the production network segmented into different zones based on security levels?

18. What is the process for making changes to network configuration?

19. Is all network traffic over public networks to the production infrastructure sent over cryptographically sound encrypted connections? (TLS, VPN, IPSEC, etc). If there are plaintext connections, what is sent unencrypted?

20. How do you keep aware of potential security vulnerabilities and threats that may affect your service?

21. How do you log and alert on relevant security events? (this includes the network and application layer)?

22. Describe or attach your Security Incident Response Program?

Shelby County Schools Information Technology
Vendor Assessment Questionnaire

23. How is your Incident Response Plan tested? Include cadence.

24. Do you have a formal service level agreement (SLA) for incident response?

25. Do you have formally defined criteria for notifying a client during an incident that might impact the security of their data or systems? What are your SLAs for notification?

Customer Facing Application Security

1) Please describe how you authenticate users: If passwords are used, describe complexity requirements, and how passwords are protected. If SSO is supported, please describe the available options

2) Does application allow user MFA to be enforced by admins?

3) Does application support IP whitelisting for user authentication?

4) Does your application support standardized roles and permissions for users (ie admin, user)?

5) Does your application enable custom granular permissions and roles to be created?

6) Which audit trails and logs are kept for systems and applications with access to customer data?

7) Does your application provide customer administrators with direct access to verbose audit logs (API, export, viewer etc)?

8) Data Retention

9) Does your application allow for custom data retention policy for customer data?

10) Does your application provide a change log? Can Shelby County Schools request copies when necessary?

11) Does your application provide a sandbox environment to customers for testing?

12) API Management
    i) How does your application store API keys?
    ii) Does application support IP whitelisting for API access?
    iii) Please describe how you authenticate users: If passwords are used, describe complexity requirements, and how passwords are protected. If SSO is supported, please describe the available options

Compliance

1) How do you conduct internal audits (audits lead by your personnel) of the service? please describe the scope, remediation process and frequency of audits.

2) How do you conduct external (third-party) audits of the service? please describe the scope and frequency of audits.

Shelby County Schools Information Technology
Vendor Assessment Questionnaire

3) Please provide a copy of the most recent report.

4) Which IT operational, security, privacy related standards, certifications and/or regulations you do comply with?

5) Please provide a copy of the most recent certifications.