SCPL Vendor Security Questions

Service Overview

Vendor business Information	
1.	Company Name
2.	Responder Name
3.	Responder Contact Information (Phone/Business Email Address)
4.	Date of Response
Company Profile	
5.	Company Website URL
6.	Service Website URL
Service Scope	
7.	Name of application or service being provided
8.	Description of application or service
9.	What technology languages/platforms/stacks/components are being utilized in the scope of the application? (AWS? MySQL? Ruby on Rails? Python? Drupal?)
Service Hosting	
10.	Is your service run from your own (a) data center, (b) the cloud, or (c) deployed-on premise only
11.	Which cloud providers do you rely on?
12.	Have you researched your cloud providers' best security practices?
13.	Which data centers/countries/geographies are you deployed in?
Vendor Supporting Documentation	
14.	In the past year, has your company preformed any Application Code Review or Penetration Testing Reports (carried out by independent third party)?
15.	Does your company have a Data Flow Diagram?
16.	In the past year, has your company completed a PCI, SOC2 type II or ISO27001 certification report?

Data Protection & Access Controls

Encryption	
17.	Do you encrypt customer data?
Data Access & Handling	
18.	Do you have capabilities to anonymize data?
19.	Do you keep sensitive data in hard copy (e.g. paper copies)?
20.	Do you have a procedure for securely destroying hard copy sensitive data?
21.	Do you support secure deletion (e.g. degaussing/cryptographic wiping) of archived or backed-up data?
22.	Describe the circumstances in which customer data is allowed leave your production systems?
Authentication	
23.	Do you have an internal password policy?
24.	Do you have complexity or length requirements for passwords?
25.	Are passwords hashed?
26.	Do employees/contractors have ability to remotely connect to your production systems? (i.e. VPN)
27.	Is MFA required for employees/contractors to log in to production systems?
28.	Do internal applications leverage SSO for authentication?
Third Party Data Processing	
29.	Do data processors (vendors) access your customer's information?
30.	Do these processors (vendors) contractually comply with your security standards for data processing?
31.	How do you regularly audit your critical vendors?
EU Data/Privacy Shield	
32.	(Only applicable if your company/data centers are based in the EU) For the provision of services, do you process EU citizens' personal data?
33.	Have you appointed a Data Protection Officer (DPO)?
34.	Do you plan on becoming Privacy Shield certified within the next 12 months?

Policies & Standards

Data Management Program	
35.	Do you have a formal Information Security Program (InfoSec SP) in place?
36.	Do you review your Information Security Policies at least once a year?
37.	Do you have a Information security risk management program (InfoSec RMP)?
38.	Do you have management support or a security management forum to evaluate and take action on security risks?
39.	Do you have a dedicated information security team?

Application Security

Authentication	
40.	Do you require password complexity?
41.	Does application allow user MFA to be enforced by admins?
42.	Does application support IP whitelisting for user authentication?
Role Based Access Control	
43.	Does your application support standardized roles and permissions for users (ie admin, user)?
44.	Does your application enable custom granular permissions and roles to be created?
Audit Logging	
45.	Are audit trails and logs are kept for systems and applications with access to customer data?
46.	Does your application provide customer administrators with direct access to verbose audit logs (API, export, viewer etc)?
Data Retention	
47.	Does your application allow for custom data retention policy for customer data?
Change Management	
48.	Does your application provide a change log?
49.	Does your application provide a sandbox environment to customers for testing?
API Management	
50.	Does your API implement rate limiting?
51.	Does your application store API keys?
52.	Does your application support IP whitelisting for API access?

Compliance

Internal Audits	
53.	Do you conduct internal audits of the service?
External Audits	
54.	Do you conduct external (third-party) audits of the service?
Privacy	
55.	Do you share customer data with, or enable direct access by, any third-party?
56.	Do you seek a right to use or own customer derived data for your own purposes?
57.	Is your Privacy Notice/ Privacy Policy externally available?

Security Measures

Security Measures	
58.	Do you perform routine network and application security testing?
59.	Are all security events (authentication events, SSH session commands, privilege elevations) in production logged?
60.	Is all network traffic over public networks to the production infrastructure sent over cryptographically sound encrypted connections? (TLS, VPN, IPSEC, etc).
61.	Are there plaintext connections?
62.	Are cryptographic frameworks are used to secure data in transit over public networks?
63.	Are cryptographic frameworks are used to secure data at rest?
64.	Are cryptographic frameworks are used to store passwords?
65.	Are any custom crypographic frameworks/implementations used? If so, have any custom cryptographic frameworks been reviewed by an independent 3rd party?
66.	Do you keep aware of potential security vulnerabilities and threats that may affect your service?
67.	Do you log and alert on relevant security events? (this includes the network and application layer)
68.	Do you have an Incident Response Plan?
69.	Do you have a formal service level agreement (SLA) for incident response?

70.	Do you have formally defined criteria for notifying a client during an incident that might impact the security of their data or systems?

Which Data Are Collected

Collected Data	
71.	When a Patron uses your service, what information are they required to give?
72.	What data types are used to login? (Library card, PIN, email, etc)
73.	Does the product have an Administrative portal? Yes/No
74.	Is the Admin portal secured with https? Yes/No
75.	List ALL patron data that can be seen in the Admin portal.
76.	How long is patron data retained in the Admin portal?
77.	How is data purged and at what frequency?
78.	Please place a check mark next to ALL of the data you collect: • Patron records • Circulation transaction logs • Overdue and billing records • Document delivery and ILL transactions • Records of access to electronic reserves • Records that support personalized services • Search histories saved beyond a session • Saved searches and sets • Files/logs of previous electronic reference queries and answers • System logs • Web server logs, including proxy servers • Personalization profiles and other service offers for personal information • Usage statistics • User-created lists • User Created Reviews