

## Vendor Security Audit

| Vendor Business Continuity / Disaster Recovery   | Satisfactory             | N/A                      | Unsatisfactory           |
|--|--------------------------|--------------------------|--------------------------|
| Vendor has a business continuity plan.   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Vendor incorporates Denial-of-Service and other cyber-attacks as part of their business continuity plan. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Vendor has an updated disaster recovery plan.  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Vendor Organizational Security   |                          |                          |                          |
| Employees of vendor complete routine cybersecurity training.   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Vendor has a formal change control process for IT  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Vendor is able to provide a company security rating.   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Vendor is able to provide a history of data breaches (if any).   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Vendor has an adequate password policy.  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Vendor General Security  |                          |                          |                          |
| Vendor installs antivirus software on core systems and endpoints.  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Vendor routinely patches systems.  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Vendor tests patches prior to implementation.  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Vendor invests in data protection and security controls.   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Vendor restricts physical access to core processing systems.   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Vendor has a process for secure disposal of equipment and media.   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Vendor's employees have unique login IDs when accessing data.  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Vendor Network Security  |                          |                          |                          |
| Vendor protects network boundaries using firewalls   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Vendor regularly performs network vulnerability scans  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Vendor uses an IDS or IPS on their network   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Vendor's remote users are required to use VPNs when accessing vendor's systems                           | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Vendor protects wireless networks (if applicable)  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |



## Vendor Security Audit

### Vendor System Security

|   |                          |                          |                          |
|---|--------------------------|--------------------------|--------------------------|
| Vendor has verified backup and recovery process.  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Vendor uses access control (Ex: RBAC).  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Vendor restricts systems that contain sensitive data to only authorized users   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Vendor securely collects, stores, or transmits PII (if applicable).   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Vendor has mitigations in place for web application exploits such as SQL Injection and XSS scripting attacks (if applicable). | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

### Vendor Incident Response

|   |                          |                          |                          |
|---|--------------------------|--------------------------|--------------------------|
| Vendor has an incident response team and they have been tested adequately.        | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Vendor continuously monitors security controls to prevent cybersecurity incidents | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Vendor has a process to remediate newly found risks.                              | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

### Vendor Auditing / Reporting / Regulations

|   |                          |                          |                          |
|---|--------------------------|--------------------------|--------------------------|
| Vendor has had an IT audit in the past 12 months.                               | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Vendor has had a penetration test in the past 12 months.                        | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Vendor is able to provide penetration test results (if applicable).             | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Vendor is able to provide an IT system outline.                                 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Vendor complies with any necessary governmental regulations (if applicable).    | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Vendor has industry standard certifications (if applicable).                    | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Vendor monitors their vendors' risk and cybersecurity standing (if applicable). | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

