Provider Security Addendum

Last Revised: 09-26-2024

Covered Services

This Security Addendum ("Addendum") describes the security-related and privacy-related audits and certifications received for, and the administrative, technical, and physical controls applicable to the Input Data information submitted by Client while using the Services. Notwithstanding the foregoing this Addendum shall not apply to professional services, support services, non-Provider applications, free trials, or training services. Capitalized terms used and not otherwise defined in this Addendum have their respective meanings assigned to such terms under the Master Services Agreement.

Information Security Management Program ("ISMP")

Provider maintains an ISMP that contains administrative, technical, and physical safeguards. The ISMP is documented and updated based on changes in legal and regulatory requirements related to privacy and data security practices and industry standards applicable to the Service. Provider's ISMP is intended to:

- Protect the integrity and availability of Input Data, and prevent the unauthorized disclosure by Provider or its agents, of Input Data in Provider's possession or control;
- Protect against anticipated threats and unauthorized disclosure of Input Data;
- Protect against unauthorized access, use, alteration, or destruction of Input Data;
- Protect against accidental loss or destruction of, or damage to, Input Data; and
- Safeguard Input Data as set forth in any applicable local, state or federal regulations by which Provider may be regulated.

---

1. **Security Standards**. Provider's ISMP includes adherence to and regular testing of the key controls, systems and procedures of its ISMP to validate that they are properly implemented and effective in addressing the threats and risks identified.

2. **Assigned Security Responsibility**. Provider assigns responsibility for the development, implementation, and maintenance of its ISMP by:

a) Designating a security official with overall responsibility; and

b) Defining security roles and responsibilities for individuals with security responsibilities.

3. **Relationship with Vendors**. Provider conducts reasonable due diligence and security assessments of applicable third party vendors ("Vendors") engaged by Provider who provide work that is material to delivery of the Services and who may store or gain access to Input Data.

4. **Background Check**. Provider performs background checks on all potential Provider employees. Potential employees must pass background check prior to being hired by Provider.

5. **Privacy & Security Awareness and Training**. Provider implements annual, mandatory privacy awareness, security awareness, and training programs for all Provider personnel that address their obligations related to the processing of personal data that is contained within Input Data.

6. **Access Controls. Provider institutes**:

a) Controls to ensure that only those Provider personnel with an actual need-to-know will have access to any Input Data;

b) Controls to ensure that all Provider personnel who are granted access to any Input Data are based on least-privilege principles;

c) Controls to require that user identifiers (User IDs) shall be unique and readily identify Provider person to whom it is assigned;

d) Password and other strong authentication controls are implemented to be in compliance with NIST guidance addressing locking out, uniqueness, reset, termination after a period of inactivity, password reuse limitations, length, and the number of invalid login requests before locking out a user;

e) Periodic access reviews to ensure that only those Provider personnel with access to Input Data still require it; and

f) Removal of access on a timely basis after termination of employment.

7. **Data Encryption**. Provider uses Internet-industry-standard secure encryption methods designed to encrypt Input Data transmitted between Provider server(s) and the Client browser(s).

8. **Secure Development Practices**. Provider follows secure application development policies, procedures, and standards that are aligned to industry-standard practices, such as the Open Web Application Security Project ("OWASP") Top 10 and SANS Top 25.

9. **Malware Control**. Provider employs current industry-standard measures to detect viruses, trojan horses, worms, logic bombs, or other harmful code or programs designed to negatively impact the operation or performance of the Service.

10. **System Monitoring**. Provider maintains security measures to monitor the network and production systems. This includes monitoring event logs on servers, disks, network appliances, and cloud services as well as additional security events. Events are assessed and remediated on a risk basis as determined by Provider.

11. **Vulnerability Management**. Provider performs various scans against code, applications, and networks to discover, prevent, and mitigate vulnerabilities. Provider engages third parties to perform network vulnerability assessments and penetration testing on an annual basis ("Vulnerability Assessments"). Vulnerabilities are remediated on a risk basis as determined by Provider.

12. **Change and Configuration Management**. Provider maintains policies and procedures for managing changes to production systems, applications, and databases. Such policies and procedures include:

a) A process for documenting, testing and approving the promotion of changes into production;

b) A process for Provider to perform security assessments of changes into production.

13. **Incident Management**. Provider has in place a security incident response plan that includes procedures to be followed in the event of a security incident impacting Provider systems, databases, and Input Data.

14. **Business Continuity Plan**. Provider has in place a documented Business Continuity Plan that has been reviewed and / or updated annually.

15. **Security Incident Management**.

a) **Notification**: Provider will notify customers within seventy-two (72) hours of confirmation of a security incident impacting their Input Data, such notification shall be in accordance with the requirements of applicable laws.

b) **Remediation**: In the event of a confirmed security incident, Provider will (i) provide any affected customer with a summary of the remediation plan to address the security incident and to mitigate the incident and reasonably prevent any further incidents, (ii) remediate the effects of the security incident in accordance with such remediation plan, and (iii) reasonably cooperate with any affected customer and any law enforcement or regulatory official investigating such security incident.