SECURITY ADDENDUM

Sigma utilizes infrastructure-as-a-service cloud providers as further described in the Agreement and/or Documentation (each, a "**Cloud Provider**") and provides the Service to Customer from a VPC hosted by the applicable Cloud Provider (the "**Cloud Environment**").

Sigma maintains a comprehensive documented security program based on NIST 800-53 (or industry recognized successor framework), under which Sigma implements and maintains physical, administrative, and technical safeguards designed to protect the confidentiality, integrity, availability, and security of the Service and Customer Data (the "**Security Program**"), including, but not limited to, as set forth below. Sigma regularly tests and evaluates its Security Program, and may review and update its Security Program as well as this Security Addendum, provided, however, that such updates will be designed to enhance and not materially diminish the Security Program.

1. **Sigma's Audits & Certifications.** The information security management system supporting the Service will be assessed by one or more independent third-party auditors in accordance with the following audits and certifications ("**Third-Party Audits**"), on at least an annual basis:

- SOC 1 Type II
- SOC 2 Type II
- SOC 3
- HIPAA

Third-Party Audits are made available to Customer as described in Section 8(b) below. To the extent Sigma discontinues a Third-Party Audit, Sigma will adopt or maintain an equivalent, industry-recognized framework.

2. **Hosting Location of Customer Data.** Sigma hosts Customer Data in its Cloud Environment located in the United States for storage and uses multiple U.S. regions for compute. Sigma may use any region in the U.S. to store or process data and Customer hereby consents to the transfer of any data to the U.S. for storage and processing purposes in accordance with the Agreement.

3. **Encryption.**
a. Encryption of Customer Data. Sigma encrypts Customer Data at-rest using AES 256-bit (or better) encryption. Sigma leverages Transport Layer Security (TLS) 1.2 (or better) for Customer Data in-transit over untrusted networks.

b. Encryption Key Management. Sigma uses its Cloud Environment's KMS with unique encryption keys per customer.

4. **System & Network Security.**

a. Access Controls. All Sigma personnel access to the Cloud Environment is via a unique user ID and consistent with the principle of least privilege. All access to the cloud console requires two-factor authentication. Access to the production environment is restricted, requires two-factor authentication.

b. Endpoint Controls. For access to the Cloud Environment, Sigma personnel use Sigma -issued laptops which utilize security controls that include, but are not limited to, (i) disk encryption, (ii) endpoint detection and response (EDR) tools to monitor and alert for suspicious activities and Malicious Code, (as defined above) and (iii) vulnerability management in accordance with the Section titled, "Vulnerability Management" below.

c. Separation of Environments. Sigma logically separates production environments from development and testing environments. The Cloud Environment is both logically and physically separate from Sigma's corporate offices and networks.

d. Firewalls / Security Groups. Sigma will protect the Cloud Environment using industry standard firewall or security groups technology with deny-all default policies to prevent egress and ingress network traffic protocols other than those that are business-required.

e. Hardening. The Cloud Environment will be hardened using industry-standard practices designed to protect it from vulnerabilities, including by changing default passwords, removing unnecessary software, disabling or removing unnecessary services, and regular patching as described in this Security Addendum.

f. Monitoring & Logging.

- *Infrastructure Logs*. Monitoring tools or services, are utilized to log certain activities and changes within the Cloud Environment. These logs are further monitored, analyzed for anomalies, and are securely stored to prevent tampering for at least one year.

g. Vulnerability Detection & Management.

- *Anti-Virus & Vulnerability Detection*. Sigma's cloud environment is built to be immutable and auto-updates and designed to prevent viruses. Known vulnerabilities are automatically patched at the host level. Sigma does not monitor Customer Data for Malicious Code.

- *Penetration Testing & Vulnerability Detection*. Sigma regularly conducts penetration tests throughout the year and engages one or more independent third parties to conduct penetration tests of the Service at least annually.

- *Vulnerability Management*. Vulnerabilities meeting defined risk criteria trigger alerts and are prioritized for remediation based on their potential impact to the Service. Upon becoming aware of such vulnerabilities, Sigma will use commercially reasonable efforts to address private and public (e.g., U.S.-Cert announced):
    - critical vulnerabilities within 7 days
    - high vulnerabilities within 30 days;
    - medium vulnerabilities within 90 days; and
    - low vulnerabilities within 180 days.

To assess whether a vulnerability is 'critical', 'high', 'medium', or low, Sigma leverages the National Vulnerability Database's (NVD) Common Vulnerability Scoring System (CVSS), or where applicable, the U.S.-Cert rating.

5. **Administrative Controls.**
a. Personnel Security. Sigma requires criminal background screening on its personnel as part of its hiring process, to the extent permitted by applicable law.

b. Personnel Training. Sigma maintains security awareness and training program for its personnel, this trailing happens during onboarding and annually thereafter. The topics in this security training include but are not limited to:

- Cyber Security;
- Information Security;
- Phishing;
- Business Email Compromise;
- Social Engineering;
- Incident Response;
- Ransomware;

- Removable Media;
- Wifi Security; and
- Privacy.

c. Personnel Agreements. Sigma personnel are required to sign confidentiality agreements. Sigma personnel are also required to adhere to Sigma's information Security Addendum.

d. Personnel Access Reviews & Separation. Sigma reviews the access privileges of its personnel to the Cloud Environment regularly, and removes access on a timely basis for all separated personnel.

e. Sigma Risk Management & Threat Assessment. Sigma's risk management process is modeled on NIST 800-53 and ISO 27001. Sigma's security team regularly reviews reports and material changes in the threat environment, and identifies potential control deficiencies in order to make recommendations for new or improved controls and threat mitigation strategies.

f. External Threat Intelligence Monitoring. Sigma reviews external threat intelligence, including US-Cert vulnerability announcements and other trusted sources of vulnerability reports. U.S.-Cert announced vulnerabilities rated as critical or high are prioritized for remediation in accordance with Section 4.7.3 (Vulnerability Management).

g. Change Management. Sigma maintains a documented change management program.

h. Vendor Risk Management. Sigma maintains a vendor risk management program for vendors that process Customer Data designed to ensure each vendor maintains security measures consistent with Sigma's obligations in this Security Addendum.

6. **Physical and Environmental Controls.**

a. Cloud Environment Data Centers. Sigma works with the Cloud Providers to ensure the Cloud Provider has appropriate physical and environmental controls for its data centers hosting the Cloud Environment. Sigma regularly reviews those controls as audited under the Cloud Provider's third-party audits and certifications. Each Cloud Provider will have a SOC 2 Type II annual audit and ISO 27001 certification, or industry recognized equivalent frameworks. Such controls, will include, but are not limited to, the following:

- Physical access to the facilities are controlled at building ingress points;
- Visitors are required to present ID and are signed in;
- Physical access to servers is managed by access control devices;
- Physical access privileges are reviewed regularly;
- Facilities utilize monitor and alarm response procedures;
- Use of CCTV;
- Fire detection and protection systems;
- Power back-up and redundancy systems; and
- Climate control systems.

b. Sigma Corporate Offices. Sigma offices host no Customer Data and have no private connectivity to our Cloud Environments. We do enforce industry standard best practices for office security included but not limited to:

- Physical access to the corporate office is controlled at building ingress points;
- Badge access is required for all personnel and badge privileges are reviewed regularly; ● Visitors are required to sign in;
- Use of CCTV at building ingress points;
- Tagging and inventory of Sigma-issued laptops and network assets;

- Fire detection and sprinkler systems; and
- Climate control systems.

7. **Incident Detection & Response.**

a. Security Incident Reporting. If Sigma becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data (a "**Security Incident**"), Sigma will notify Customer without undue delay, and in any case, where feasible, notify Customer within 48 hours after becoming aware.

b. Investigation. In the event of a Security Incident as described above, Sigma will promptly take reasonable steps to contain, investigate, and mitigate any Security Incident. Sigma in its sole discretion may engage a third party incident response/forensics company to help with the mitigation/investigation.

c. Communication and Cooperation. Sigma will provide Customer timely information about the Security Incident to the extent known to Sigma, including, but not limited to, the nature and consequences of the Security Incident, the measures taken and/or proposed by Sigma to mitigate or contain the Security Incident, the status of Sigma's investigation, a contact point from which additional information may be obtained, and the categories and approximate number of data records concerned. Notwithstanding the foregoing, Customer acknowledges that because Sigma personnel do not have visibility to the content of Customer Data, it will be unlikely that Sigma can provide information as to the particular nature of the Customer Data, or where applicable, the identities, number, or categories of affected data subjects. Sigma's communications with Customer in connection with a Security Incident will not be construed as an acknowledgment by Sigma of any fault or liability with respect to the Security Incident.

8. **Customer Rights & Shared Security Responsibilities.**

a. Penetration Testing. Customer may provide a written request for a copy of Sigma's most recent penetration ("**Pen Test**") by submitting such request via a support ticket. Sigma will provide a copy of such Pen Test within thirty (30) days of Customer's request.

b. Documentation. Upon written request and at no additional cost to the Customer, Sigma will provide Customer with access to reasonably requested documentation that evidences Sigma's compliance with its obligations under this Security Addendum in the form of (i) Sigma's SOC 1 Type II and/or SOC 2 Type II audit report, (ii) Sigma's SOC 3 audit report and any other certifications detailing Sigma's compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), (iii) Sigma's most recently completed industry standard security questionnaire, such as a SIG or CAIQ, and (iv) data flow diagrams for the Service ("**Security Reports**").

c. Sensitive Customer Data. Customer Data should not include any sensitive data (as defined by applicable data protection laws); it is the Customer's responsibility to ensure that any Customer Data containing content regulated by PCI-DSS, FedRAMP, or containing any similarly regulated content is in compliance with the appropriate regulatory requirements and controls. Customer acknowledges and Sigma makes no warranty and has no third party verified compliance certifications around PCI-DSS, and/or FedRAMP.

d. Shared Security Responsibilities. Without diminishing Sigma's commitments in this Security Addendum, Customer agrees:

- Sigma does not assess or monitor the content of Customer Data to identify information subject to any specific legal, regulatory or other requirements and Customer is responsible for making appropriate use of the Service to ensure a level of security appropriate to the particular content of Customer Data; and

- to be responsible for managing and protecting its User roles and credentials, including but not limited to (i) requiring that all Users keep credentials confidential and not share such information with unauthorized parties, (ii) reporting to Sigma any suspicious activities in the account or if a user credential has been compromised, (iii) appropriately configuring User and role-based access controls, including scope and duration of User access, taking into account the nature of its Customer Data, and (iv) maintaining appropriate password uniqueness, length, complexity, and expiration.

e. GDPR / CCPA. As Sigma does not access the Customer Data it is the Customer's responsibility to submit deletion requests for the appropriate data subject. Sigma shall promptly notify Customer if Sigma receives a request from a data subject for access to, correction, amendment or deletion of such data subject's Personal Data. Sigma shall not respond to any such request without Customer's prior consent except to confirm that the request relates to the Customer.