

SECURITY POLICY

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 another 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, Customer Data, User Information, and Input Data (the "**Security Program**"). Sigma regularly tests and evaluates the Security Program and may review and update the Security Program as well as this Security Policy, 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 auditing bodies in accordance with the following audits, regulatory standards, and certifications ("**Third-Party Audits**") on at least an annual basis:

- SOC 1 Type II
- SOC 2 Type II
- SOC 3
- HIPAA
- ISO 27001
- ISO 27017
- ISO 27018
- ISO 27701

Third-Party Audits are made available to Customer as described in Section 9(b) below.

2. **Hosting Location of Customer Data.** Sigma processes Customer Data, User Information, and Input Data in its Cloud Environment located in the United States and uses multiple U.S. regions for compute. Sigma may use any region in the U.S. to store (if applicable), transmit, or process Customer Data, User Information, and Input Data and Customer hereby consents to the transfer of any data to the U.S. for such purposes. For customers domiciled outside the United States of America, and who may have specific local regulatory requirements, the Service is also available to process Customer Data, User Information, and Input Data in Cloud Environments located in Canada, Europe, Australia/APAC, and the United Kingdom. Sigma conducts privacy and transfer impact assessments to ensure compliance with local and regional regulatory requirements in order for Sigma to store, transfer, or process Customer Data and Input Data in these locations. Current Cloud Environment locations and regions can be viewed [here](#).

3. Encryption.

a. Encryption of Customer Data. Sigma encrypts Customer Data, User Information, and Input Data at-rest using AES 256-bit (or better) encryption. Sigma uses industry-standard encryption techniques to encrypt Customer Data in transit, leveraging by default Transport Layer Security (TLS) 1.2 (or better) for Customer Data, User Information, and Input Data in-transit over untrusted networks.

b. Encryption Key Management. Sigma uses secure Cloud Environment's key management service (KMS) with unique encryption keys per customer.

4. System & Network Security.

a. Access Controls. Any Sigma personnel that must access to the Cloud Environment in the course of their duties access such Cloud Environment via a unique user ID, consistent with the principle of least privilege. All access to the Cloud Environment requires two-factor authentication. Access to the production environment within the Cloud Environment is restricted and provisioned via a zero-trust network access (ZTNA) solution which is monitored and logged. Sigma's enterprise password management system requires minimum password parameters.

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 4.g titled, “Vulnerability Detection & Management” below.

c. Separation of Environments. Within the Cloud Environment, 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 protects 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 is hardened using industry-standard practices designed to protect such environment from vulnerabilities, including by changing default passwords, removing unnecessary software, disabling or removing unnecessary services, and regular patching as described in this Security Policy.

f. Monitoring & Logging. Monitoring tools or services are utilized to log certain activities and changes within the Cloud Environment. Such logs are further monitored, analyzed for anomalies, and are securely stored for at least one (1) year in a manner designed to prevent tampering.

g. Vulnerability Detection & Management.

Anti-Virus & Vulnerability Detection. The Cloud Environment is built to be immutable, auto-updates itself, and is designed to prevent Malicious Code (as such term is defined in the Agreement). Known vulnerabilities are automatically patched at the host level.

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 uses the National Vulnerability Database’s (NVD) Common Vulnerability Scoring System (CVSS), where applicable, the U.S.-Cert rating and Sigma Internal risk rating.

h. *External and Internal Penetration Testing*. Sigma regularly conducts internal penetration tests throughout the year and engages an independent third party to conduct penetration tests on Sigma Cloud Infrastructure and Web application Service at least annually.

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 a security awareness and training program for its personnel, this training 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 adhere to Sigma's Information Security Policy.

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.g(Vulnerability Detection & 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, User Information, and Input data designed to ensure each vendor maintains security measures consistent with Sigma's obligations in this Security Policy.

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's corporate offices do not host Customer Data, User Information, or Input data and have no private connectivity to the Cloud Environments. Nevertheless, Sigma enforces industry standard best practices for office security including 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.

8. **Data Deletion**. Upon termination of the Agreement and written request from Customer, Sigma will delete all User Information within thirty (30) days of such request by Customer. Such a request must be made in writing by an authorized representative of Customer.

9. Business Continuity and Disaster Recovery (BCDR). Sigma ensures its BCDR through regional and zonal resiliency and redundancy. Sigma commits to a Recovery Point Objective (RPO) of 24 hours and Recovery Time Objective (RTO) of 8-12 hours in AWS. To ensure compliance with these BCDR objectives, Sigma performs an annual BCDR test and provides the results on its [Trust Center](#).

9. Customer Rights & Shared Security Responsibilities.

a. Penetration Testing. Customers 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 Customers' request by making such report available via the Sigma Trust Center

b. Customer Audit Rights. Customer's audit rights hereunder will be as set forth in the DPA.

c. Sensitive Customer Data. Customer Data and Input data should not include any sensitive data; 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 processed in compliance with the appropriate regulatory requirements and controls. Customer acknowledges and Sigma makes no warranty and has no third party verified compliance certifications regarding PCI-DSS, and/or FedRAMP. In addition, use of the Service to meet requirements of HIPAA may require additional controls from Customer.

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

i. Sigma does not assess or monitor the content, accuracy, or legality of Customer Data or Input data to identify information subject to any specific legal, regulatory, or other requirements and Customer is responsible for ensuring a level of security appropriate to the particular content of Customer Data; and

ii. it is 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.