InfoSum

Security Policy

This InfoSum Security Policy (the "Security Policy") outlines the technical and procedural measures that InfoSum undertakes to protect Customer Data from unauthorized access or disclosure. This Security Policy is referenced in and made a part of the Terms of Service of the Platform ("Terms of Service"). In the event of any conflict between the terms of the Terms of Service and this Security Policy, this Security Policy shall govern. Capitalized terms used but not defined in this Security Policy have the meanings set forth in the Terms of Service.

1. Customer Data Access and Management

1.1. The Customer controls access to its Datasets via User IDs, passwords (with strong password enforcement) and optionally with 2-factor authentication tokens.

1.2. InfoSum Personnel may not access unencrypted Uploaded Data without the Customer's consent. "InfoSum Personnel" means InfoSum employees and individual subcontractors.

1.3. InfoSum uses Uploaded Data only as necessary to provide the Platform and as set out in clause 4.1 of the Terms of Service.

1.4. Uploaded Data is stored only in a dedicated virtual server hosted on AWS, which is allocated exclusively to the Customer (a "Bunker").

1.5. InfoSum shall create and maintain flow diagram(s) indicating how Uploaded Data flows through the Platform. InfoSum shall provide such flow diagram(s) upon Customer's reasonable request.

2. Handling of Uploaded Data

2.1. All traffic within Platform including the initial HTTP transmission of Uploaded Data to the Bunker is secured and encrypted by a TLS 1.2 secured session that utilises the Elliptical Curve Diffie Hellman Cipher suites (AES256-GCM-SHA384, CHACHA20-POLY1305-SHA256 & AES128-GCM-SHA256). Bunkers enforce HTTPS Strict Transport Security and support forward secrecy as well as secure renegotiation.

2.2. Uploaded Data is held in the Bunker initially in a raw state pending normalisation. Access to the Bunker is secured in accordance with section 1 above, with no other access available to the other InfoSum systems, except for:

2.2.1. the Address Mapper which is a service located in the InfoSum Cloud that parses postal address data to return a UDPRN into the Bunker.

2.2.2. the results of an Identity Query (e.g. a list of IDs) are sent to the InfoSum Cloud for onward transmission at the direction of the Customer. This data is encrypted when at rest in the InfoSum Cloud using AES encryption ciphers, as defined in the FIPS197 standard

Additionally the connection between the Customer's browser and the Bunker is secured with HTTPS.

2.3. Upon completion of the normalisation process all Identifying Data within the Uploaded Data is hashed according to FIPS PUB 108-4 standards and the raw Identifying Data is deleted. the Uploaded Data may only be accessed by InfoSum's data analysis systems.

2.4. The hashed Identifying Data remains in the Bunker. To provide the Platform, InfoSum's data analysis systems transmit a probabilistic representation of a set of hashed Identifying Data and/or Non-Identifying Data to InfoSum's cloud system and to the Bunkers of any third party who has permission or has granted a permission to run a query.

2.5. Where Bunkers are hosted by InfoSum, then they are deployed into a dedicated, isolated subnet within a private VPC supernet. Layer 3 IP routing between Bunkers is prohibited; layer 3 reachability between the Bunker and the InfoSum cloud service is achieved with a VPC peering connection. All traffic entering or leaving a Bunker is subject to both dedicated and inherited AWS security groups to restrict what TCP traffic can enter or leave a Bunker.

3. InfoSum Service Infrastructure Access Management

3.1. Access to the systems and infrastructure that support the InfoSum Service is restricted to InfoSum Personnel who require such access as part of their job responsibilities. All of those personnel are trained in accordance with paragraph 10 below.

3.2. Unique User IDs are assigned to InfoSum Personnel requiring access to the InfoSum servers that support the Platform.

3.3. Server password policy for the Platform in the production environment adheres to UK Government National Cyber Security Centre recommendations and industry best practises.

3.4. Access privileges of all InfoSum Personnel are monitored and adjusted accordingly as circumstances require.

3.5. User access privileges to the systems and infrastructure that support the Platform are reviewed quarterly.

3.6. Access attempts to the systems and infrastructure that support the Platform are logged and monitored.

4. Risk Management

4.1. InfoSum manages risk in accordance with industry best practices as detailed by the ISO27001 and SOC2 standards.

4.2. InfoSum conducts risk assessments of various kinds throughout the year, including self- and third-party assessments and tests, automated scans, and manual reviews.

4.3. Results of assessments, including formal reports as relevant, are reported to the Director of Security and reviewed by senior management together with recommendations for new or improved controls and threat mitigation strategies.

4.4. Changes to controls and threat mitigation strategies are evaluated and prioritized for implementation on a risk-adjusted basis.

4.5. Threats are monitored through various means, including threat intelligence services, vendor notifications, and trusted public sources.

5. Vulnerability Scanning and Penetration Testing

5.1. Vulnerability scans are automatically performed weekly on the systems that operate and manage the InfoSum Service. The vulnerability database is updated regularly.

5.2. Scans that detect vulnerabilities meeting InfoSum-defined risk criteria automatically trigger notifications to security personnel.

5.3. Potential impacts of vulnerabilities that trigger alerts are evaluated by staff.

5.4. Vulnerabilities that trigger alerts and have published exploits are reported to the Director of Security, who determines and supervises appropriate remediation action.

5.5. Security management monitors or subscribes to trusted sources of vulnerability reports and threat intelligence.

5.6. Penetration tests by an independent third party expert shall be conducted at least annually.

5.7. Penetration tests performed by InfoSum Security are performed regularly throughout the year.

6. Remote Access & Wireless Network

6.1. All access to the InfoSum infrastructure requires authentication through a secure connection using approved methods such as VPNs and enforced with mutual certificate authentication and/or multi-factor authentication.

6.2. InfoSum maintains a strict policy of not storing Account Data or Uploaded Data (where access to InfoSum Personnel has been granted by the Customer) on local desktops, laptops, mobile devices, shared drives, removable media, as well as on public facing systems that do not fall under the administrative control or compliance monitoring processes of InfoSum.

7. Location of Data in the Platform

7.1. Uploaded Data is stored in AWS servers physically located in the UK.

8. System Event Logging

8.1. Monitoring tools and services are used to monitor systems including network, server events, and AWS API security events, availability events, resource utilization and internal service performance metrics.

8.2. InfoSum infrastructure security event Logs are centralised in an industry standard Security Information and Event Management system (SIEM). SEIM logs are stored for 12 months.

9. System Administration and Patch Management

9.1. InfoSum maintains system administration procedures for systems that access Uploaded Data that meet or exceed industry standards, including without limitation, system hardening, system and device patching (operating system and applications).

9.2. InfoSum Security reviews various vulnerability announcements weekly and assess their impact to InfoSum based on a InfoSum-defined risk criteria, including applicability and severity.

9.3. Applicable security updates rated as “high” or “critical” are addressed within 24 hours of the patch release.

10. InfoSum Security Training and InfoSum Personnel

10.1. InfoSum maintains a security awareness program for InfoSum Personnel, which provides initial education, ongoing awareness and individual InfoSum Personnel acknowledgment of intent to comply with InfoSum’s corporate security policies. All Personnel are contractually obliged to abide by the InfoSum Information Security Policy and undertake training on security procedures.

10.2. All InfoSum Personnel acknowledge they are responsible for reporting actual or suspected security incidents or concerns, thefts, breaches, losses, and unauthorized disclosures of or access to Customer Data.

10.3. All InfoSum Personnel are required to satisfactorily complete quarterly security and data protection training.

10.4. InfoSum performs criminal background screening as part of the InfoSum hiring process of Personnel to the Security Team, to the extent legally permissible.

10.5. InfoSum will ensure that its subcontractors, vendors, and other third parties that have direct access to the Customer Data in connection with the Platform adhere to the data security standards of ISO27001 and SOC2

11. Physical Security

11.1. The InfoSum Service is hosted in AWS and all physical security controls are managed by AWS. InfoSum reviews the AWS SOC 2 Type 2 report annually to ensure appropriate physical security controls with regard to:

11.1.1. Visitor management including tracking and monitoring physical access.

11.1.2. Physical access point to server locations are managed by electronic access control devices.

11.1.3. Monitor and alarm response procedures.

11.1.4. Use of CCTV cameras at facilities.

11.1.5. Video capturing devices in data centres with 90 days of image retention.

12. Notification of Security Breach

12.1. A "Security Breach" is (a) the unauthorized access to or disclosure of Uploaded or Account Data, or (b) the unauthorized access to the systems within the Platform that transmit or analyse Uploaded or Account Data.

12.2. InfoSum will notify Customer in writing within forty eight (48) hours of a confirmed Security Breach.

12.3. Such notification will describe the Security Breach and the status of InfoSum's investigation.

12.4. InfoSum will take appropriate actions to contain, investigate, and mitigate the Security Breach.

13. Customer Responsibilities

13.1. The Customer is responsible for managing its own user accounts and roles within the Platform and for protecting its own account and user credentials. The Customer will comply with the Terms of Service as well as all applicable laws.

13.2. The Customer will promptly notify InfoSum if a user credential has been compromised or if the Customer suspects possible suspicious activities that could negatively impact security of the Platform or the Customer's account.

13.3. The Customer may not perform any security penetration tests or security assessment activities without the express advance written consent of InfoSum.