INFOSUM SECURITY POLICY

This InfoSum Security Policy (the "Security Policy") outlines the technical and procedural measures that InfoSum undertakes to protect Customer data (which comprises both Account and Uploaded Data) from unauthorized access or disclosure. This Security Policy is referenced in and made a part of the Terms of Service of the InfoSum Platform ("Platform Terms of Service"). In the event of any conflict between the terms of the Platform 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 Platform 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. Passwords used to access the InfoSum Platform (including Datasets) are stored in hashed form in accordance with industry best practice.

1.2.   InfoSum Personnel may not access 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 5.1 of the Platform Terms of Service.

1.4.   Uploaded Data is stored only in a dedicated virtual server hosted on Amazon Web Services (AWS), which is allocated exclusively to the Customer (a "Bunker"). Uploaded Data is stored or processed only using AWS services independently certified to conform with ISO 27001 and SOC 2.

1.5.   Each Dataset is stored in its own separate Bunker, which only the Customer may access (unless the Customer provides consent as described in 1.2 above).

1.6.   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 and between the Customer's browser and the Bunker 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. Bunkers enforce HTTPS Strict Transport Security and support forward secrecy as well as secure renegotiation.

2.2.   All physical storage used by the Bunker is protected by full disk encryption.

2.3.   If the Customer no longer requires a Bunker, or if the Customer ends their use of the InfoSum Platform, the data stored within the Bunker is immediately and permanently deleted. The encryption key is also destroyed, meaning that the data could not be accessed even in the unlikely event that it were recovered from physical media.

2.4.   Access to the Bunker is secured in accordance with section 1 above, with no other access available to the other InfoSum systems, except for:

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

2.4.2.   where the Customer has specifically requested this functionality, 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

2.5.   Uploaded Data is held in the Bunker initially in a raw state pending normalisation. 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.

2.6.   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.

2.7.   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 Platform Infrastructure Access Management

3.1.   Access to the systems and infrastructure that support the InfoSum Platform 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 11 below.

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

3.3.   InfoSum Personnel's access to servers in the production environment is only using cryptographic keys in accordance with industry best practices, with 2-factor authentication as an additional protection.

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 is certified as compliant with ISO 27001 (view our certificate). This certification independently confirms that InfoSum manages risk in accordance with international best practice; that it has a detailed, documented Information Security Management System; that policies are regularly reviewed and continuously improved; and that a focus on security is driven from the very top of the organisation.

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 Security Review Board 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 on the systems that operate and manage the InfoSum Platform. Port scans are performed weekly, and more detailed scans are performed monthly. 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 InfoSum Personnel.

5.4. Vulnerabilities that trigger alerts and have published exploits are reported to the Head of Security and Director of Engineering, who determine and supervise appropriate remediation action.

5.5. Penetration tests by an independent third party expert are conducted at least twice a year, and generally on a quarterly basis.

5.6. 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 by default, although other AWS locations may be used at the request of a customer.

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 maintains a documented patch management process, which ensures that patches are applied within a timeframe commensurate to their impact within the specific environment of the InfoSum Platform.

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

10. InfoSum Development Practices

10.1. In developing and enhancing the InfoSum Platform, InfoSum follows written development practices which ensure that security features are preserved.

10.2. All modifications to the InfoSum Platform are tested in separate environments before they are deployed to the InfoSum Platform in production.

10.3. All modifications to the InfoSum Platform must be reviewed by at least two people (including the person who made the change). Technical controls are in place to ensure this policy is correctly applied.

10.4. Any open-source software used within the InfoSum Platform is individually assessed and signed off, to ensure that it follows satisfactory security principles and that there are no licensing implications which might affect the security of Customer data.

11. InfoSum Security Training and InfoSum Personnel

11.1. 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 InfoSum Personnel are obliged to abide by the InfoSum Information Security Policy and undertake and satisfactorily complete annual training on security procedures.

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

11.3. To the extent legally permissible, InfoSum performs criminal background screening as part of the hiring process of Personnel who will have login access to the systems and infrastructure which operate the InfoSum Platform in production.

11.4. Any contractors or other contingent workers used by InfoSum are subject to the same vetting processes, and the same security policies, as any other InfoSum Personnel.

12.   Physical Security

12.1.   The InfoSum Platform 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:

12.1.1.   Visitor management including tracking and monitoring physical access.

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

12.1.3.   Monitor and alarm response procedures.

12.1.4.   Use of CCTV cameras at facilities.

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

13.   Notification of Security Breach

13.1.   A "Security Breach" is (a) the unauthorized access to or disclosure of the Customer's data, or (b) the unauthorized access to the systems within the Platform that transmit or analyse the Customer's data.

13.2.   InfoSum will notify Customer in writing within forty eight (48) hours of a confirmed Security Breach affecting their data.

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

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

14.   Customer Responsibilities

14.1.   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 Platform Terms of Service as well as all applicable laws.

14.2.   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 InfoSum Platform or the Customer's account.

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

Updated: 17 April 2019