SMART 5 Consulting Limited

Information Security Policy

t: +44(0) 20 3686 6135
m: +44(0) 780 944 9726 [Syed]
w: https://www.smart5.co.uk
e: syed@smart5.co.uk,info@smart5.co.uk

SMART 5 Consulting Limited. Registered in England and Wales. Company Registration No. 12281263, Registered Office: 23, Quarles Park Road, Romford, RM6 4DE.

Information Security Policy

Introduction

SMART5 considers protection of Customer Data a top priority. As further described in this SMART5 Information Security Policy, SMART5 uses commercially reasonable organizational and technical measures designed to prevent unauthorized access, use, alteration or disclosure of Customer Data stored on systems under SMART5's control. SMART5 maintains these security measures in accordance with ISO 27001, 27017 and 27018.

1. Customer Data and Management. SMART5 limits its personnel's access to Customer Data as follows:

1.1. Requires unique user access authorization through secure logins and passwords, including multi-factor authentication for Cloud Hosting administrator access and individually-assigned Secure Socket Shell (SSH) keys for external engineer access;

1.2. Limits the Customer Data available to SMART5 personnel on a "need to know" basis;

1.3. Restricts access to SMART5's production environment by SMART5 personnel on the basis of business need;

1.4. Encrypts user security credentials for production access; and

1.5. Prohibits SMART5 personnel from storing Customer Data on electronic portable storage devices such as computer laptops, portable drives and other similar devices.

1.6. SMART5 logically separates each of its customers' data and maintains measures designed to prevent Customer Data from being exposed to or accessed by other customers.

2. Data Encryption. SMART5 provides industry-standard encryption for Customer Data as follows:

2.1. Implements encryption in transport and at rest;

2.2. Uses strong encryption methodologies to protect Customer Data, including AES 256-bit encryption for Customer Data stored in SMART5's production environment; and

2.3. Encrypts all Customer Data located in cloud storage while at rest.

3. Network Security, Physical Security and Environmental Controls

3.1. SMART5 uses firewalls, network access controls and other techniques designed to prevent unauthorized access to systems processing Customer Data.

3.2. SMART5 maintains measures designed to assess, test and apply security patches to all relevant systems and applications used to provide the Services.

3.3. SMART5 monitors privileged access to applications that process Customer Data, including cloud services.

3.4. The Services operate on Amazon Web Services ("AWS") and Google Cloud ("GCS") and are protected by the security and environmental controls of Amazon and Google, respectively. Detailed information about AWS security is available at https://aws.amazon.com/security/ and http://aws.amazon.com/security/sharing-the-security-responsibility/. For AWS SOC Reports, please see https://aws.amazon.com/compliance/soc-faqs/. Detailed information about GCS security is available at https://cloud.google.com/docs/tutorials#security.

3.5. Customer Data stored within AWS or GCS is encrypted at all times. AWS and GCS do not have access to unencrypted Customer Data.

4. Independent Security Assessments. SMART5 periodically assesses the security of its systems and the Services as follows:

4.1. Annual detailed security and vulnerability assessments of the Services conducted by independent third-party security experts that include a code analysis and a comprehensive security review. SMART5 shall attest to Customer the date of the most recent security and vulnerability assessment at Customer's reasonable request.

4.2. SMART5 hires accredited third parties to perform audits and to attest to various compliance and certifications annually including ISO 27001, 27017, and 27018.

4.3. Bi-annual penetration testing of SMART5 systems and applications to test for exploits including, but not limited to, XSS, SQL injection, access controls, and CSRF.

4.4. Monthly vulnerability scanning.

5. Incident Response. If SMART5 becomes aware of unauthorized access or disclosure of Customer Data under its control (a "Breach"), SMART5 will:

5.1. Take reasonable measures to mitigate the harmful effects of the Breach and prevent further unauthorized access or disclosure.

5.2. Upon confirmation of the Breach, notify Customer in writing of the Breach without undue delay. Notwithstanding the foregoing, SMART5 is not required to make such notice to the extent prohibited by Laws, and SMART5 may delay such notice as requested by law enforcement and/or in light of SMART5's legitimate needs to investigate or remediate the matter before providing notice.

5.3. Each notice of a Breach will include:

5.3.1. The extent to which Customer Data has been, or is reasonably believed to have been, used, accessed, acquired or disclosed during the Breach;

5.3.2. A description of what happened, including the date of the Breach and the date of discovery of the Breach, if known;

5.3.3. The scope of the Breach, to the extent known; and

5.3.4. A description of SMART5's response to the Breach, including steps SMART5 has taken to mitigate the harm caused by the Breach.

6. Business Continuity Management

6.1. SMART5 maintains an appropriate business continuity and disaster recovery plan.

6.2. SMART5 maintains processes to ensure failover redundancy with its systems, networks and data storage.

7. Personnel Management

7.1. SMART5 performs employment verification, including proof of identity validation and criminal background checks for all new hires, including contract employees, in accordance with applicable law.

7.2. SMART5 provides training for its personnel who are involved in the processing of the Customer Data to ensure they do not collect, process or use Customer Data without authorization and that they keep Customer Data confidential, including following the termination of any role involving the Customer Data.

7.3. SMART5 conducts routine and random monitoring of employee systems activity.

7.4. Upon employee termination, whether voluntary or involuntary, SMART5 immediately disables all access to SMART5 systems, including SMART5's physical facilities.