CreatorIQ

TECHNICAL AND ORGANIZATIONAL SECURITY SCHEDULE 5

Information Security Management System
ISO/IEC 27001

1.1

17.09.2020

Table of Content

1. Technical and organizational security measures

This Schedule 5 describes certain technical and organizational security measures that SocialEdge has implemented in accordance with applicable laws, rules, treaties, and governmental regulations, including without limitation applicable Data Protection Laws as they apply to the provision of the Services and as directed by Customer. All terms, capitalized or otherwise, that are used in this Schedule 5 that are defined in Schedule 4, shall have the meanings ascribed to such terms in Schedule 4. Taking into account the state of the art, the costs of implementation and the nature, scope, content and purpose of the processing, SocialEdge represents and warrants that it has implemented the data security measures described below.

1.1. Physical Access All databases, application servers and related hardware used to power SocialEdge systems are hosted in secure AWS and Azure clouds. Physical access to those devices is controlled by Amazon and Microsoft respectively and conforms with state-of-the-art best practices. All SocialEdge data and processing resources are secured by Virtual Private Networks (VPNs). Access to SocialEdge VPNs is limited to SocialEdge personnel that requires this access to perform their job functions.

1.2. Virtual Access Technical and organizational measures to prevent unauthorized persons from virtually accessing SocialEdge's systems, including:

- 1.1.1. Establishing user identification and authentication procedures;
- 1.1.2. Establishing ID/password security procedures (special characters, minimum length, change requirements);
- 1.1.3. Ensuring that admission to the data processing systems is only possible after identification and authentication using the correct identification code and password for the particular system;
- 1.1.4. Using automatic blocking (e.g., password or timeout);
- 1.1.5. Monitoring intrusion attempts and automatically turning off user ID upon several erroneous passwords attempts;
- 1.1.6. Creating one master record per user, user master data procedures, per data processing environment;
- 1.1.7. Using firewalls and proxy servers; and
- 1.1.8. Implementing encryption and pseudonymization as appropriate. Suitability of an encryption technology is evaluated by reference to its protective purpose.

2. Data access

Technical and organizational measures to ensure that persons entitled to use a data processing system gain access only in accordance with their access rights, and that personal data cannot be read, copied, modified, or deleted without authorization, including: Establishing written internal policies and procedures;

- 2.1. Ensuring that personal data necessary for the performance of the particular task is limited within the systems and applications by a corresponding role and authorization framework, which allows access to employees on a "need to know" basis, ensuring that each role has only such access rights as are necessary to fulfil the task to be performed by that specific person;
- 2.2. Establishing control authorization schemes;
- 2.3. Establishing differentiated access rights (profiles, roles, transactions and objects);

- 2.4. Monitoring and logging of access;
- 2.5. Encryption and pseudonymization, as appropriate. Suitability of an encryption technology is evaluated by reference to its protective purpose.

3. Disclosure and transmission

The measures necessary to ensure security of personal data during processing and transmission are described in SocialEdge's information security policy and are implemented in accordance with a risk-based security classification system. SocialEdge transfers Covered Customer Data to third parties in accordance with the Customer's instructions and this Agreement and enters into a written agreement with such third parties in accordance with applicable Data Protection Laws. Covered Customer Data will not be stored or processed using non-secure or non-professional systems (e.g., public cloud systems).

4. Other controls

Technical and organizational measures to monitor whether personal data may have been entered, changed, or removed (deleted), and by whom, from data processing systems, including logging and reporting systems and audit trails and documentation. Technical and organizational measures to ensure that personal data are processed solely in accordance with the instructions of Customer, including the Agreement, and this Schedule. Technical and organizational measures to ensure that personal data are protected against accidental destruction or loss (physical/logical), including:

- 4.1. Establishing backup procedures;
- 4.2. Mirroring hard disks;
- 4.3. Ensuring uninterruptible power supply;
- 4.4. Using remote storage;
- 4.5. Using anti-virus/firewall systems; and
- 4.6. Establishing a disaster recovery plan. Technical and Organizational Security - Schedule 5, ensures the availability of its data processing systems themselves in accordance with the necessary security level by corresponding security measures. Technical and organizational measures to ensure that personal data collected for different purposes can be processed separately, including:
- 4.7. Separating databases;
- 4.8. Establishing parameters for limitation of use;
- 4.9. Segregating functions (production/testing); and
- 4.10. Establishing procedures for separate storage, amendment, deletion; transmission of data for different purposes.

5. Information Classification

- **5.1. Owners and Production Information.** All electronic information managed and processed by SocialEdge must have a designated Owner. Production information is information routinely used to accomplish business objectives. Owners should be at the Director level or above. Owners are responsible for assigning appropriate sensitivity classifications as defined below. Owners do not legally own the information entrusted to their care. They are instead designated members of the Senior or Executive Management team who act as stewards, and who supervise the ways in which each type of information is used and protected.
- **5.2. Public.** Information Assets are classified as "Public" if the Company makes the explicit decision to share them with the public. This classification may only be applied by business units that are authorized to do so.
- **5.3. Internal Use.** This category applies to the majority of the Information Company manages; this is Information required and created as part of our day-to-day activities. Internal Use Information may be shared with Company employees and contractors and with third parties external to the Company. However, when we

share information or communicate with third parties outside the Company, it is always important to consider the possible consequences or repercussions for the Company. It is our obligation to protect Company Information and Company corporate reputation.

- **5.4. Confidential.** This category covers Sensitive Information that could cause damage if shared with unauthorized people. Information Assets that contain Personal Data (including name, phone number, physical address, email address, and any other data relating to an identifiable individual) must be classified as Confidential – Personal Data. Confidential Information may be shared with Company employees and contractors; and third parties external to Company that have signed a nondisclosure agreement (NDA). The owner and the recipients of “Confidential” Information Assets distributed in paper assume responsibility for limiting the distribution. In electronic form, “Confidential” Information must be subject to technical controls, when available, ensuring that the owner controls who has access to the Information. And all information that relates to the provision or receipt of the Platform or Services or either party's financial condition, operations or business, and which is clearly identified as confidential at the time of disclosure, (b) for Customer as the Receiving Party: the Technology, the Documentation, and the User IDs (all as defined herein), and (c) for SocialEdge as the Receiving Party.
- **5.5. Highly Confidential.** This covers very Sensitive Information that would cause damage if shared with unauthorized people. It is recommended to consult legal before classifying an Information Asset as Highly Confidential. Information Assets that contain Sensitive Personal Data should be classified as Highly Confidential – Sensitive Personal Data. Highly Confidential Information Assets may be shared with Company employees and contractors; and third parties external to Company that have signed a non-disclosure agreement approved by the legal function. Highly Confidential Information Assets in electronic form must be subject to additional technical controls, when available, ensuring that only predefined individuals can access the Information. Highly Confidential Information Assets in paper form must be shared only with a pre-defined group of individuals.
- **5.6. Owners and Access Decisions.** Data Owners must make decisions about who will be permitted to gain access to information, and the uses to which this information will be put. IS must take steps to ensure that appropriate controls are utilized in the storage, handling, distribution, and regular usage of electronic information, and that these controls are monitored and kept up to date