Spredfast Security Standards

Capitalized terms not otherwise defined in this document have the meanings assigned to them in the applicable Spredfast Customer Agreement.

1. Information Security Program. Spredfast will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) satisfy the Security Objectives, (b) identify reasonably foreseeable and internal risks to security and unauthorized access to the Spredfast platform, and (c) minimize security risks, including through risk assessment and regular testing. Spredfast will designate one or more employees to coordinate and be accountable for the information security program. The information security program will include the following measures:

1.1 Network Security. Spredfast will maintain access controls and policies to manage access allowed to the Spredfast network from each network connection and User, including the use of firewalls or functionally equivalent technology and authentication controls. Spredfast will maintain corrective action and incident response plans to respond to potential security threats.

1.2 Physical Security

1.2.1 Physical Access Controls. Spredfast is hosted within Amazon Web Services ("AWS"); AWS manages the physical security of the data center(s). Physical components of the Spredfast network are housed in nondescript facilities (the "AWS Facilities"). Physical barrier controls are used to prevent unauthorized entrance to the AWS Facilities both at the perimeter and at building access points. Passage through the physical barriers at the Facilities requires either electronic access control validation (e.g., card access systems, etc.) or validation by human security personnel (e.g., contract or in-house security guard service, receptionist, etc.).

1.2.2 Limited AWS Employee and Contractor Access. Spredfast is hosted within AWS; AWS manages access to the physical facilities. AWS provides access to AWS Facilities to those employees and contractors who have a legitimate business need for such access privileges. When an employee or contractor no longer has a business need for the access privileges assigned to him/her, the access privileges are promptly revoked, even if the employee or contractor continues to be an employee of AWS or its affiliates.

1.2.3 Physical Security Protections. All AWS Facility access points (other than main entry doors) are maintained in a secured (locked) state. Access points to the AWS Facilities are monitored by video surveillance cameras designed to record all individuals accessing the Facilities. AWS also maintains electronic intrusion detection systems designed to detect unauthorized access to the Facilities, including monitoring points of vulnerability (e.g., primary entry doors, emergency egress doors, roof hatches, dock bay doors, etc.) with door contacts, glass breakage devices, interior motion-detection, or other devices designed to detect individuals attempting to gain access

to the Facilities. All physical access to the Facilities by employees and contractors is logged and routinely audited.

1.3 Spredfast Application Security

1.3.1 Access Controls. The Spredfast Software-as-a-Service platform will be electronically accessible to employees, contractors and any other person as necessary to provide the Services. Spredfast will maintain access controls and policies to manage what access is allowed to the Spredfast platform from each User, including the use of authentication controls and privileged account policies. Spredfast will maintain corrective action and incident response plans to respond to potential security threats.

1.3.2 Encryption. Spredfast uses industry standard algorithms to encrypt data in transit and at rest (e.g. TLS, AES-256, etc). Encryption keys are provided through AWS tools and are centrally managed by Spredfast staff. Spredfast regularly evaluates encryption standards and updates the algorithms in use as necessary.

1.3.3 Vulnerability Management. Spredfast follows a code development process that integrates data privacy, security, and quality concerns. Spredfast contracts with independent third parties to perform penetration testing and vulnerability assessments of the service. Vulnerabilities are remediated according to severity pursuant to Spredfast's Service Level Agreement. P1 (critical) issues are addressed promptly until resolved, P2 (high) issues are worked during business hours until resolved, and P3 (all others) issues are prioritized into the next development sprint.

1.3.4 Customer Vulnerability Testing. Customer may request the results of the penetration testing and vulnerability assessment described in Section 1.3.3 from security@spredfast.com once in a twelve (12) month period. . Spredfast does not allow additional testing or assessments to be performed.

2. Continued Evaluation. Spredfast will conduct periodic reviews of the security of its Spredfast network and adequacy of its information security program as measured against industry security standards and its policies and procedures. Spredfast will continually evaluate the security of its Spredfast network and associated Services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.

3. Security Breach Notification.

3.1 Security incident. If Spredfast becomes aware of an actual breach of security of the Spredfast Security Standards or any unauthorized access to Spredfast's SaaS Platform, leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to any Customer Data ("Security Incident"), Spredfast will without undue delay: (a) notify affected Customers of the Security Incident; and (b) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

3.2 Customer Assistance. To assist Customer in relation to any personal data breach notifications Customer is required to make under the GDPR, Spredfast will include in the notification under section 3.1(a) such information about the Security Incident as Spredfast is reasonably able to disclose to Customer, taking into account the nature of the Services, the information available to Spredfast, and any restrictions on disclosing the information, such as confidentiality.

3.3 Unsuccessful Security Incidents. Customer agrees that:

(i) an unsuccessful Security Incident will not be subject to this Section 3. An unsuccessful Security Incident is one that results in no unauthorized access to Customer Data or to any of Spredfast's equipment or facilities storing Customer Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents; and

(ii) Spredfast's obligation to report or respond to a Security Incident under this Section 3 is not and will not be construed as an acknowledgement by Spredfast of any fault or liability of Spredfast with respect to the Security Incident.

3.4 Communication. Notification(s) of Security Incidents, if any, will be delivered to one or more of Customer's administrators by any means Spredfast selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information by notifying security@spredfast.com of any changes..

3.5 Privacy Impact Assessment and Prior Consultation. The information made available by Spredfast under Section 4 is intended to assist Customer in complying with Customer's obligations under the GDPR in respect of data protection impact assessments and prior consultation.

4. Certifications and Audits.

4.1 Spredfast SSAE 18 SOC 2 Report. Spredfast possesses a current SSAE 18 SOC 2 report and agrees to maintain an information security program for the Services that complies with the SSAE 18 SOC 2 standards for the establishment, implementation, control, and improvement of the Spredfast security standards.

4.2 Audits. Spredfast uses external auditors to verify the adequacy of its security measures, including the security of the infrastructure within a private cloud in AWS from which Spredfast provides the Services. This audit: (a) will be performed at least annually; (b) will be performed according to SSAE 18 SOC 2 standards; (c) will be performed by independent third party security professionals at Spredfast's selection and expense; and (d) will result in the generation of an audit report ("Report"), which will be Spredfast's Confidential Information. If Customer's Agreement does not include a provision protecting Spredfast Confidential Information, then Reports will be made available to Customer subject to a mutually agreed upon non-disclosure agreement covering the Report (an "NDA").

4.3 Audit Reports. At Customer's written request, Spredfast will provide, no more than once in a twelve (12) month period, Customer with a confidential Report so that Customer can reasonably verify Spredfast's compliance with its obligations under this Addendum. The Report will constitute Spredfast's Confidential Information under the confidentiality provisions of the Agreement or the NDA, as applicable.

4.4 Independent Determination. Customer is responsible for reviewing the information made available by Spredfast relating to data security and making an independent determination as to whether the Services meets Customer's requirements and legal obligations as well as Customer's obligations under this Agreement.

4.5 Customer Audits. Customer agrees to exercise any right it may have to conduct an audit or inspection, including under the Standard Contractual Clauses if they apply, by instructing Spredfast to carry out the audit described in Section 4.2 at its own expense. If the Standard Contractual Clauses apply, nothing in this Section 10 varies or modifies the Standard Contractual Clauses nor affects any supervisory authority's or data subject's rights under the Standard Contractual Clauses.

5. Data Retention and Destruction

5.1 Data Retention. The SaaS Platform processes social data for various functions and allows direct data entry for certain features. Customer Data is retained according to the following timelines:

(i) Inbound social content, both public and private, is rendered inaccessible after 90 days (it is no longer indexed) and is permanently deleted after 25 months.

(ii) Social metrics (public data) is available for 13 months before deletion.

(iii) Notes, used during moderation and publishing functions, entered directly into the SaaS Platform are retained indefinitely.

(iv) Social content published through the Spredfast service is retained indefinitely.

5.2 Data Destruction at Termination. Spredfast functions as a Data Processor of social content. The social data lives on the relevant Social Media Network. Spredfast does not have access to delete this content, from the native social network upon termination of the Agreement.

Upon termination of the Agreement, Spredfast will make the data described in Section 5.1 unreadable. The company account will be locked and no user accounts may be added to it (including internal Spredfast accounts). The data is encrypted using AES-256 and is dead data in our system.