441 9th Ave, 12 floor
New York, NY 10001

Acceptable Use Policy (AUP)

1. Definitions

To the extent not already defined in the applicable Master Agreement, the following definitions shall apply:
"**Connected Services**" means the various channels and integrations supported by the Platform that Customer connects to, or authorizes a third party to connect to, through the Platform, including the social media services.
"**Connected Services Authorization**" means the authorization relating to the Customer's Connected Services accounts, which enable the Platform to interact with Customer's Connected Services accounts.
"Connected Services Terms" the terms of service or use or any other terms and conditions governing or conditioning use of Connected Services, together with any associated rules and policies of any Connected Service.
"Customer Care Data" means any material that is submitted to the Platform by a person other than a Customer User through the Connected Services that the Customer has integrated into the Sprinklr Platform for purposes of customer care and support (including, where applicable under the Order Form, voice data).
"Customer Content" means any material that is (i) entered into the Sprinklr Account by Customer, an Agency or employee on behalf of or under the direction of Customer (ii) generated by Customer, an Agency or employee on behalf of or under the direction of Customer, through use of the Sprinklr Platform, or (iii) published through the Sprinklr Account to the Connected Services for which Sprinklr has Connected Services Authorization.
"**Personal Data**" means "personal data,"
"Personal Information" or an equivalent term, as defined by any applicable laws and regulations applicable to the Processing of Personal Data under the Master Agreement ("Data Protection Legislation") to the extent such data or information is accessed, collected, stored, transmitted, processed, hosted, used, handled, or disposed of by Sprinklr in connection with the Master Agreement.
"Platform" means Sprinklr's proprietary customer experience software service, accessed by Customer via the internet, as specified in an applicable Order Form. Platform includes Updates made during the Term.
"Sprinklr Account" means Customer's password restricted account to access and use the Platform.

2. Compliance

Customer must comply with all applicable laws, regulations, and all Connected Services Terms with respect to its usage of the Platform, including its processing of any Personal Data via the Platform. Customer is responsible for ensuring data subjects have sufficient notice or, where required, have provided consent, for the processing, use, disclosure, or transfer of any information from the Connected Services related to an identified or identifiable person on the Platform, as required by applicable law, including Data Protection Legislation, or any relevant Connected Services Terms. Customer is responsible for all activity conducted under its Sprinklr Account, regardless of knowledge or intent, as well as all Customer Content that is entered through its Sprinklr Account on the Platform. By its integration and use of Connected Services (including operation thereof via the Platform), Customer hereby instructs Sprinklr to receive and/or to transmit (as applicable) any Personal Data in Customer Content to the fullest extent required to enable Sprinklr to provide its Services.

3. Customer Content

Customer Content may not: (i) be defamatory, harmful to minors, obscene, indecent, pornographic, libelous, threatening, harassing, false, misleading or inaccurate; (ii) contain or cause to be placed on Sprinklr's or any other third party's systems any Trojan horses, worms, viruses or programming routines intended to interfere, damage, corrupt, surreptitiously intercept or expropriate any system, data or personal information; (iii) violate any applicable local, state, federal or foreign law, rule or regulation, including Data Protection Legislation); (iv) violate any Connected Services Terms; (v) infringe or violate any third party rights; or (vi) contain any health, medical, financial, credit card, or other payment information or any information of any person under the age of 13. Customer Content that does not comply with any one or more of the clauses (i) – (vi) above is referred to as "Prohibited Information." Customer is

responsible for reviewing and approving all Customer Content created or entered through or in its Sprinklr Account (including via the Connected Services). Customer is solely responsible for monitoring the communications it receives from users of the Connected Services that are processed through the Platform and for promptly removing any Prohibited Information from the Platform, except where Customer is under a legal duty to retain Prohibited Information as may be included in Customer Care Data, in which case Customer shall retain the minimal amount of Prohibited Information required to comply with the legal duty, and shall take the necessary measures to limit the access to such information on a strict need-to-know basis and ensure the data is backed up in a secondary location. Sprinklr does not pre-screen Customer Content, however Sprinklr has the right, but not the obligation, to remove Prohibited Information from, or refuse to process any Prohibited Information on, the Platform and to make it unavailable through the Platform, as Sprinklr may reasonably determine. In addition, upon notice, Sprinklr may terminate or suspend use by any authorized user that created or entered or processed such Prohibited Information (including through use of a Connected Service).

4. Protected Health Information

Customer shall inform Sprinklr if there will be any Protected Health Information" in the Customer Content. To the extent the Customer informs Sprinklr and executes a Business Associate Agreement, Customer Content is then permitted to include Protected Health Information," as defined by HIPAA so long as such Customer Content is processed exclusively through the HIPAA Eligible Sprinklr Services, as outlined at trust.sprinklr.com. Customer shall ensure that it has all rights, consents, approvals, and authorizations to include such Protected Health Information" in Customer Content and Customer's use of such information in the Connected Services shall comply with all applicable law, including but not limited to HIPAA, the Business Associate Agreement, and all other relevant sections of the applicable Master Agreement.

5. Account

Customer may only access and use the Platform through the Sprinklr Account and agrees to provide and maintain accurate and current Sprinklr Account information and Connected Services Authorization. Customer is responsible for adding authorized users to its Sprinklr Account, for maintaining the confidentiality of all Sprinklr Account passwords, for ensuring that each Sprinklr Account password is used only by the authorized user, for ensuring that Sprinklr Accounts and passwords are not shared, and for maintaining the security of its Sprinklr Account and of the equipment needed to connect to, access or use the Platform and the Connected Services. Customer shall limit access to the Platform only to authorized persons and will promptly disable all access to the Sprinklr Account by any employee, contractor or Customer representative who is no longer authorized to use the Platform.