441 9th Avenue, 12th Floor
New York, NY 10001

Sprinklr Enterprise Security Addendum

This Enterprise Security Addendum ("ESA") applies to all data processed on behalf of our customers in the Sprinklr Platform and in the provision of the Sprinklr Services, including any Sprinklr owned or leased servers used to host Customer's data.

The following technical and organizational measures are implemented by Sprinklr, in accordance with industry standards, to ensure an appropriate level of security related to use of the Sprinklr Platform. For access to documentation evidencing each of the measures listed below, including relevant certifications, please visit Sprinklr's Trust Center.

Information Security Program

Sprinklr has a dedicated security team led by Sprinklr's Chief Information Security Officer (CISO), chartered to define, supervise implementation of, and monitor all relevant security policies, standards, and controls (the "Security Team"). The Security Team is supported by Sprinklr's Board of Directors and the Executive Leadership Team and is independent from Sprinklr's Research & Development team, Information Technology team, and other operational teams. By independently validating the implementation of application security controls and reporting the outcome to Sprinklr leadership, the Security Team ensures proper accountability and a risk-informed decision process for maintaining and evolving the security program. In addition, Sprinklr's internal Governance, Risk, and Compliance function, alongside third-party auditors, provides oversight on Sprinklr's overall security posture and internal controls for risk management.

Security Manual

The Security Manual, available upon request, is maintained by the Security Team and provides an overview of all applicable security policies, controls, and procedures, as well as processes for the management of actual or reasonably suspected security incidents, including through (a) training personnel with access to the Sprinklr Platform and Customer data to recognize and report potential or actual security incidents; and (b) conducting post-incident reviews of events and actions taken.

Audit and Assurance

The Sprinklr Platform undergoes annual, independent audit and assurance assessments according to risk-based plans and policies. Sprinklr maintains the following: Reports – SOC 2 Type II, and SOC 3 and Certification – ISO 27001:2013, or an industry equivalent.

Regular Risk Assessment of Information Security Program

Sprinklr conducts information security risk assessments annually, or whenever there is a material change in Sprinklr's business or technology practices that materially impacts the privacy, confidentiality, security, integrity, or availability of Customer data. These risk assessments include the validation of administrative, procedural, and technical controls and are conducted by independent third parties (e.g., third-party assessors and penetration testers) or the independent internal Security Team. Remediation of any material findings is tracked and validated.

Controls

Physical Access and Environmental Controls

For all production systems, Sprinklr leverages our public cloud provider capabilities for the implementation and maintenance of physical controls to protect servers, networks, and facilities from unauthorized access. Controls include secure building with multiple secure access zones; secure perimeters; 24/7 video surveillance; on-site guard service; suitable environmental protections including climate-controlled data rooms and uninterruptible power sources; and other services as required by applicable regulations or requirements. Sprinklr periodically validates the suitability of these controls through third-party security audit reports and/or vendor audits. For more information on which cloud providers are used by Sprinklr, please refer to our subprocessor list, available at www.sprinklr.com/subprocessors.

Logical Access Controls

Logical access to Sprinklr servers is limited to only those Sprinklr personnel who have the need and approval to access the servers directly. The Sprinklr Platform is set behind perimeter security controls jointly managed by the cloud provider and Sprinklr. Sprinklr designed security controls for Internet traffic to traverse load balancers or similar technology. Sprinklr continuously monitors the key parameters for Sprinklr Services for unusual access activity.

Network Transport Controls

Sprinklr has implemented industry standard security controls designed to protect all Customer data in transit from attacks against confidentiality or integrity. These controls include the implementation of applicable network protocols, encryption schemes, hashing of data, cryptographic signature, etc. Sprinklr's cryptographic keys used for Network Transport Security Controls are managed using industry standard practices.

Data Storage Controls

All media containing Customer data is protected from unauthorized physical access. Customer data at rest is encrypted using industry standard encryption mechanisms. Cryptographic keys are managed by Sprinklr in accordance with industry standard practices. Sprinklr's third party cloud hosting providers utilize NIST SP800-88 data destruction techniques. Customer data is deemed irrecoverable once deleted.

Authentication Controls

Sprinklr implements industry standard identity governance processes and authentication mechanisms to ensure that only authorized users can interact with systems. This includes multi-factor authentication, single-sign-on architecture where technically feasible, and timely user provisioning and deprovisioning processes. Where feasible, user actions, including successful and unsuccessful login attempts, user identifier, IP address, date, and time stamp are logged. It is mandatory for all customers to integrate their SSO solution with their Sprinklr instance or utilize Sprinklr's 2FA capabilities for all user accounts to securely authenticate into the Sprinklr platform.

Data Access Controls (Authorization)

Access to specific data, systems, or services is limited to user roles based on job responsibilities following the principle of least privilege as possible. Role Based Access Control ("RBAC") is used where feasible, and periodic access recertifications are in place.

Remote Access Controls

Remote access to Sprinklr's backend systems is restricted to authorized personnel based on their role. The access follows the principle of a multi-tiered security control approach which includes employees with backend access to connect to the bastion host from Sprinklr's VPN which is whitelisted, and device validation is performed in order to connect. Once authenticated, SSH is utilized to access the bastion host. Username and password are required to authenticate to the bastion with two factor authentication as the final step**.**

Communication Controls

Sprinklr verifies and establishes the parties to which personal data have been or may be transmitted or otherwise made available. Subprocessors used by Sprinklr are initially - and afterwards periodically - assessed for data security and privacy practices consistent with Sprinklr's own data security and privacy practices. Sprinklr does not sell, furnish, or otherwise share Customer data without the consent of the Customer or the data subject, as applicable.

Input Controls

Sprinklr limits, monitors, and logs where applicable how data is entered into our systems. Standard software development security controls are in place to sanitize potentially harmful external input. This includes industry standard controls designed to prevent the introduction or spread of malicious software ("Malware").

Processing Controls

All processing by Sprinklr is conducted on behalf of and at the instruction of the Customer. Processes and technical controls in place to enforce this are reviewed on a periodic basis.

Availability Controls

All data critical for the operation of Sprinklr's Platform, as well as Customer data, is protected by multiple controls to ensure continuous protection of such data such as runtime mechanisms including redundant storage of operational data and multiple backups (with the exception of Sprinklr Services that, by design, do not persist Customer data), and other industry standard controls as applicable.

Personnel Security and Training

Sprinklr requires that all employees complete a successful background check prior to beginning their employment at Sprinklr. Subject to local appliable laws, such background checks assess:

- Criminal history
- Prior Employment verification
- Education Verification
- Social Security Verification
- National Sex Offender Registry
- Global Sanctions & Enforcement
- Physical Address Verification

Employees also undergo mandatory security awareness training upon hire and at least annually thereafter.

Application Security and Vulnerability Management

Sprinklr has a rigorous security testing and vulnerability management program in place. Application level and infrastructure level penetration testing is performed using an external party on an annual basis and identified vulnerabilities are remediated in accordance with Sprinklr's vulnerability management standard using the following timeline:

Rating	Remediation Timeline
Critical	7 Days
High	30 Days
Moderate	90 Days
Low	180 Days

Sprinklr follows a Secure Development Lifecycle ("SDL") process based on industry standard guidelines and practices. Sprinklr follows a risk-based approach to identify security issues in SDL for major code releases utilizing a combination of periodic static testing, dynamic testing, and other techniques as appropriate. Identified issues are managed by the Security Team. Developers undergo secure code training which incorporates OWASP Top 10 guidelines. Source code management and deployment follow segregation of duties and least privilege principles. Sprinklr maintains separate environments for development, testing, QA, and production. Production data is not stored or used in testing environments.

Tools or techniques used to assess security or attack computer systems or networks (i.e. vulnerability scanners, port scanners, penetration tools, etc.) without Sprinklr's authorization are strictly prohibited.

Incident Response

Sprinklr maintains an Incident Response Plan ("IR Plan") that is managed by a dedicated team and reviewed and tested annually. IR training is conducted at least once a year. Identified incidents are assigned a severity level, triaged, and managed through resolution, as well as post-mortem, where needed based on the severity of the incident. The IR Plan defines response times according to incident severity level, roles and responsibilities, and incident declaration procedures. Depending on the severity level, the IR Sprinklr's Crisis Management Team, which includes Sprinklr Legal and Communications teams, as well as other relevant stakeholders across the company to support risk assessments, devise and execute on remediation plans, provide ongoing monitoring of issues, and communicate, where needed, with customers in accordance with the notification provisions of the Agreement and DPA. Notifications for personal data breaches are governed by Sprinklr's DPA.

Data and Systems Recovery

Sprinklr's production environment utilizes an Active-Active High-Availability setup across multiple data centers per region, spaced according to industry standards for primary and backup locations. This ensures near real-time recovery in the event of a data center outage, achieving an "inner-regional" RTO/RPO of under 1 minute within the primary region. Disaster recovery procedures are only triggered in the event of a total region loss, where multiple data centers are impacted, at which point a 24-hour "cross-regional" RTO/RPO of 24 hours applies. The associated processes are periodically reviewed and tested where applicable.

Integrity

Sprinklr has implemented protective controls designed to ensure that stored data cannot be corrupted by means of a malfunctioning of the system. Such controls include system redundancy, cryptographic hashing, checksumming, and other industry standard measures as applicable. Once data is entered into our systems, Sprinklr has appropriate development and operational controls to ensure the data quality of our systems.

Secure Configuration

Sprinklr leverages industry standard security baseline definitions and vendor best practices to ensure suitable secure configuration of Sprinklr production cloud environments. Sprinklr assesses all cloud environments on a regular basis against security requirements and remediates issues according to the Sprinklr Vulnerability Management standard.

Endpoint Protection

Sprinklr is cloud-based, and Customer data is stored on an isolated cloud instance Storage of Customer data on employee devices is prohibited. Sprinklr employees laptops are pre-configured and centrally managed by Sprinklr's IT Team. The pre-configuration includes endpoint detection and response and antivirus agent, full disk encryption, write-disabled USB, inactivity logout, minimum 14-character password, firewall, and revoked administrative rights. Connection to Sprinklr's backend systems is restricted to corporate issued laptops.