SERVICENOW LOOM SECURITY GUIDE

ServiceNow recently acquired Loom Systems Inc. and Loom Systems Ltd. (collectively "**Loom**"), which provides an AI based log analysis SaaS offering to customers ("**Loom Product**"). This Loom Security Guide ("**Loom Security Guide**") applies when Customer has purchased a subscription deployment of the Loom Product that is hosted by Microsoft. In the event of any conflict or inconsistency between this Loom Security Guide and the terms of the Customer agreement with ServiceNow ("**Agreement**"), this Loom Security Guide shall control with respect to Loom Products. All capitalized terms not defined in this Loom Security Guide will have the meaning given to them in the Agreement, as applicable.

1. **LOOM SECURITY PROGRAM.** While providing the Loom Product, ServiceNow will maintain a written information security program of policies, procedures and controls governing the processing, storage, transmission and security of Customer Data within the Loom Products (the "**Loom Security Program**"). The Loom Security Program includes standard practices designed to protect Customer Data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. ServiceNow may periodically review and update the Loom Security Program to address new and evolving security technologies, changes to industry standard practices, and changing security threats, although no such update will materially reduce the commitments, protections or overall level of service provided to Customer as described herein.
2. **PHYSICAL, TECHNICAL, AND ADMINISTRATIVE SECURITY MEASURES**
   - **2.1 PHYSICAL SECURITY MEASURES**
     - **2.1.1 DATA CENTER FACILITIES**. **(a)** Physical access restrictions and monitoring that may include a combination of any of the following: multi-zone security, man-traps, appropriate perimeter deterrents (e.g. fencing, berms, guarded gates), on-site guards, biometric controls, CCTV, and secure cages; and **(b)** fire detection and fire suppression systems both localized and throughout the data center floor.
     - **2.1.2 SYSTEMS, MACHINES AND DEVICES**. (a) Physical protection mechanisms; and (b) entry controls to limit physical access.
     - **2.1.3 MEDIA**. Industry standard destruction of sensitive materials before disposition of media storing Customer Data.
   - **2.2 TECHNICAL SECURITY MEASURES**
     - **2.2.1 ACCESS ADMINISTRATION**. Access to the Loom Product by ServiceNow employees and contractors is protected by authentication and authorization mechanisms. User authentication is required to gain access to the Loom Product. Access privileges are based on job requirements and are revoked upon termination of employment or consulting relationships. Production infrastructure includes appropriate user account and password controls (e.g., complex passwords with expiration dates, and a two-factored authenticated connection) and is accessible for administration.
     - **2.2.2 SERVICE ACCESS CONTROL**. The Loom Product provides user and role-based access controls. Customer is responsible for configuring such access controls within its instance.
     - **2.2.3 FIREWALL SYSTEM.** An industry-standard firewall is installed and managed to protect the Loom Product by residing on the network to inspect all ingress connections routed to the Loom environment.
     - **2.2.4 CHANGE CONTROL.** ServiceNow will evaluate changes to platform, applications, and production infrastructure to minimize risk and to confirm that such changes are implemented in accordance with the standard operating procedure.
     - **2.2.5 DATA SEPARATION.** Customer Data shall be maintained within a logical single-tenant architecture on multi-tenant cloud infrastructure that is logically and physically separate from ServiceNow's corporate infrastructure.

2.3 ADMINISTRATIVE SECURITY MEASURES

2.3.1 PERSONNEL SECURITY. ServiceNow performs background screening on all employees and all contractors who have access to Customer Data in accordance with ServiceNow's then-current applicable standard operating procedure and subject to Law (as defined in the Agreement).

2.3.2 SECURITY AWARENESS AND TRAINING. ServiceNow maintains a security and privacy awareness training program that includes appropriate training of ServiceNow personnel on the Security Program. Training is conducted at time of hire and periodically throughout employment at ServiceNow.

3. SERVICE CONTINUITY

3.1 **DATA MANAGEMENT**. ServiceNow will host Customer's access to and use of purchased instances of the Loom Product in data centers that attained SSAE 18 Type 2 attestations or have ISO 27001 certifications (or equivalent or successor attestations) for the Subscription Term specified on the Order Form. Each data center includes full redundancy (N+1) and fault tolerant infrastructure for electrical, cooling and network systems. The deployed servers are enterprise scale servers with redundant power to ensure maximum uptime and service availability. Each Customer's application is supported by a network configuration with multiple connections to the Internet.

3.2 **PERSONNEL.** In the event of an emergency that renders the customer support telephone system unavailable, all calls are routed to an answering service that will transfer to the ServiceNow telephone support representative, geographically distributed to ensure business continuity for support operations.