SERVICENOW SWEAGLE DATA SECURITY GUIDE

This ServiceNow Sweagle Data Security Guide ("**Sweagle DSG**") describes the measures ServiceNow takes to protect User Data and Customer Data (as applicable and as defined in the applicable Agreement) within the Sweagle Product (as defined below). In the event of any conflict or ambiguity between the terms of this Sweagle DSG and the terms of the Agreement, this Sweagle DSG shall control for the Sweagle Product. All capitalized terms not defined in this Sweagle DSG will have the meaning given to them in the Agreement, as applicable. As used herein and for purposes of this Sweagle DSG, "**Agreement**" means the applicable underlying agreement between Customer and ServiceNow which, by way of example, could be an agreement governing the evaluation of the Sweagle Product or an agreement governing the purchase of a subscription SaaS offering from ServiceNow for the Sweagle Product. "**Law**" means any applicable law, rule, statute, decree, decision, order, regulation, judgment, code, and requirement of any government authority (federal, state, local, or international) having jurisdiction. **"Sweagle Products**" means the Sweagle software as a service (SaaS) offering ordered by Customer under a ServiceNow Order Form.

1. SWEAGLE SECURITY PROGRAM

While providing the Sweagle Product, ServiceNow will maintain a written information security program of policies, procedures and controls governing the processing, storage, transmission and security of User Data and Customer Data, as applicable, within the Sweagle Products (the "**Sweagle Security Program**"). The Sweagle Security Program includes standard practices designed to protect User Data and Customer Data, as applicable, from accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. ServiceNow may periodically review and update the Sweagle 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 you 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 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 User Data and Customer Data, as applicable.

2.2 TECHNICAL SECURITY MEASURES

2.2.1 ACCESS ADMINISTRATION. Access to the Sweagle Product by ServiceNow employees and contractors is protected by authentication and authorization mechanisms. User authentication is required to gain access to the Sweagle 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 Sweagle 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 Sweagle Product.

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. User Data and Customer Data, as applicable, shall be maintained 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 User Data and Customer Data, as applicable, in accordance with ServiceNow's then-current applicable standard operating procedure and subject to Law.

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 Sweagle 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 or the Evaluation Term, as applicable and 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.