DATA SECURITY ADDENDUM

1. SECURITY PROGRAM

While providing the Subscription Service, ServiceNow will ensure there is a written information security program of policies, procedures and controls aligned to the ISO27001 Series, or substantially equivalent standard, governing the processing, storage, transmission and security of Customer Data (the "Security Program"). The Security Program will include industry-standard practices designed to protect Customer Data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. ServiceNow updates the Security Program to address new and evolving security technologies, changes to industry standard practices, and changing security threats, provided that no such update will materially reduce the overall level of commitments or protections provided to Customer as described herein.

1.1 SECURITY ORGANIZATION. There will be a Chief Information Security Officer, or equivalent executive, that is designated as responsible for coordinating, managing, and monitoring the information security function, policies, and procedures.

1.2 POLICIES. The information security policies will be: (i) documented; (ii) reviewed and approved by management, including after material changes; and (iii) published, and communicated to personnel, and contractors, including appropriate ramifications for non-compliance.

1.3 RISK MANAGEMENT. There will be information security risk assessments performed as part of a risk governance program that is established with the objective to regularly test, assess and evaluate the effectiveness of the Security Program. Such assessments will be designed to recognize and assess the impact of risks and implement identified risk reduction or mitigation strategies to address new and evolving security technologies, changes to industry standard practices, and changing security threats.

2. CERTIFICATIONS AND AUDITS

2.1 CERTIFICATIONS AND ATTESTATIONS. ServiceNow will establish and maintain sufficient controls to meet certification and attestation for the objectives stated in ISO27001, ISO27018, SSAE 18 / SOC 1 and SOC 2 Type 2 (or equivalent standards) for the Security Program. At least once per calendar year, an assessment against such standards and audit methodologies by an independent third-party auditor will be obtained for environments where Customer Data is stored.

2.2 AUDIT. ServiceNow will allow for and contribute to audits that include inspections by granting Customer access to reasonable and industry recognized documentation evidencing the policies and procedures governing the security and privacy of Customer Data and the Security Program through a self-access documentation portal ("ServiceNow CORE") and at no additional costs ("Audit"). The information available in ServiceNow CORE will include documentation evidencing the Security Program, inclusive of the privacy policies and procedures regarding Personal Data Processed, as well as copies of certifications and attestation reports (including audits) listed above. To the extent that Customer has not reasonably been able to satisfy its audit requirements by following the procedure outlined in this Clause, ServiceNow will provide Customer with such further assistance as may reasonably be required (in accordance with the assistance obligations described herein) to substantially satisfy such requirements.

2.3 OUTPUT. Upon Customer’s request, ServiceNow and Customer may schedule a mutually convenient time to discuss the Audit. In the event the Audit has any findings of material noncompliance with the Data Processing Addendum or this Data Security Addendum ("DSA"), then ServiceNow will promptly address such findings of noncompliance. ServiceNow may, in its sole discretion and consistent with industry and ServiceNow’s standards and practices, make commercially reasonable efforts to implement Customer’s suggested improvements noted in the Audit to improve ServiceNow’s Security Program. The Audit and the results derived therefrom are Confidential Information of ServiceNow.

3. PHYSICAL, TECHNICAL, AND ORGANIZATIONAL SECURITY MEASURES

3.1 PHYSICAL SECURITY MEASURES.
3.1.1. DATA CENTER FACILITIES. The data center facilities will include: (1) physical access restrictions and monitoring that will 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 (2) fire detection and fire suppression systems both localized and throughout the data center floor.

3.1.2. MEDIA. For deletion of data, an industry standard such as NIST 800-88 (or substantially equivalent) will be used for the deletion of sensitive materials, including Customer Data, before final disposition of such media.

3.2. TECHNICAL SECURITY MEASURES.

3.2.1. ACCESS ADMINISTRATION. Access by personnel to Customer Data will be conducted in a manner that: (i) is protected by authentication and authorization mechanisms; (ii) requires personnel to be assigned a unique user account; (iii) restricts the sharing of individual user accounts; (iv) requires strong authentication with complex passwords; (v) ensures accounts are lock-out enabled; (vi) requires access over a VPN; (vii) requires access privileges be based on job requirements limited to that necessary for the applicable personnel to undertake their duties; (viii) ensures access is revoked upon termination of employment or consulting relationships; and (ix) requires access entitlements be reviewed by management quarterly.

3.2.2. LOGGING AND MONITORING. The production infrastructure log activities will be centrally collected, secured in an effort to prevent tampering, and monitored for anomalies by a trained security team.

3.2.3. FIREWALL SYSTEM. Firewall technology will be installed and managed to protect systems and inspect ingress connections. Managed firewall rules will be reviewed in accordance with then-current operating procedures, which will be reviewed no less frequently than quarterly.

3.2.4. VULNERABILITY MANAGEMENT. Vulnerability scans will be performed within the environment to determine potential vulnerabilities in accordance with then-current security operating procedures, which will be at least quarterly. When software vulnerabilities are revealed and addressed by a vendor patch, the patch will be obtained from the applicable vendor and applied within an appropriate risk-based timeframe in accordance with the then-current vulnerability management and security patch management standard operating procedure and only after such patch is tested and determined to be safe for installation in production systems.

3.2.5. ANTIVIRUS. Antivirus, anti-malware, and anti-spyware software will be updated on regular intervals and centrally logged.

3.2.6. CHANGE CONTROL. Changes to the environment will be reviewed to minimize risk. Such changes will be implemented in accordance with then-current standard operating procedure.

3.2.7. CONFIGURATION MANAGEMENT. Standard hardened configurations for the system components within the environment will be maintained using industry standard hardening guides, such as guides from the Center for Internet Security.

3.2.8. DATA ENCRYPTION IN TRANSIT. Industry standard encryption will be used to encrypt Customer Data in transit over public networks.

3.2.9. DATA ENCRYPTION AT REST. The encryption of Customer Data at rest will be determined by Customer and, if encrypted, will be encrypted as determined by Customer according to the applicable offerings.

3.2.10. ILICIT CODE AND SECURE SOFTWARE DEVELOPMENT. ServiceNow will follow the secure software development and code review practices described in this section to prevent harm from malware, such as from viruses, worms, date bombs, time bombs, or shut down devices. Software will be developed using secure application development policies and procedures aligned with industry standard practices such as the OWASP Top Ten (or a substantially equivalent standard). Personnel responsible for secure application design and development will receive appropriate training regarding secure application development practices.
3.2.11. **SECURE CODE REVIEW.** A combination of static and dynamic testing of code will be performed prior to the release of such code to Customers. Vulnerabilities will be addressed in accordance with the then-current software vulnerability management program. To address vulnerabilities where code has been made available to Customers, software patches will be regularly made available to Customers.

3.3 **ORGANIZATIONAL SECURITY MEASURES.**

3.3.1. **PERSONNEL SECURITY.** Background screening will be performed on all employees and all contractors who have access to Customer Data in accordance with applicable standard operating procedure and subject to applicable Law.

3.3.2. **SECURITY AWARENESS AND TRAINING.** Security and Privacy awareness training and education will be provided to employees and contractors who have access to Customer Data. Such training will be conducted at time of hire and at least annually throughout employment.

3.3.3. **VENDOR RISK MANAGEMENT.** Any vendor that accesses, stores, processes or transmits Customer Data will be assessed to ensure it has appropriate security and privacy controls.

3.3.4. **SOFTWARE AND ASSET INVENTORY.** An inventory of the software components (including, but not limited to, open-source software) used in the environment will be maintained.

3.3.5. **WORKSTATION SECURITY.** Security mechanisms on personnel workstations, including firewalls, anti-virus, and full disk encryption with a minimum of AES 128-bit encryption will be implemented and maintained. Personnel will be restricted from disabling security mechanisms.

4. **SERVICE CONTINUITY**

4.1 **DATA LOCATION.** ServiceNow will host the purchased instances in data centers located in the geographic region specified on the Order Form which have attained SSAE 18 Type 2 attestations or have ISO 27001 certifications (or equivalent or successor attestations or certifications).

4.2 **DATA BACKUP.** Back-ups will be performed of all Customer Data in accordance with the then-current operating procedure available in the CORE Portal.

4.3 **DISASTER RECOVERY.** An Information Security Contingency Plan (ISCP) to address disaster recovery will be maintained that is consistent with industry standards for the environment and will: (i) test the ISCP at least once every year; (ii) make available summary test results that will include the actual recovery point and recovery times; and (iii) document any action plans within the summary test results to promptly address and resolve any deficiencies, concerns, or issues that prevented or may prevent the environment from being recovered in accordance with the ISCP.

4.4 **BUSINESS CONTINUITY.** A business continuity plan ("BCP") will be maintained to minimize the impact from an event to ServiceNow’s provision and support of the Subscription Services. The BCP will: (i) include processes for protecting personnel and assets and restoring functionality in accordance with the time frames outlined therein; and (ii) be tested annually and updated based on any deficiencies identified during such tests.

5. **MONITORING AND INCIDENT MANAGEMENT**

5.1 **INCIDENT MONITORING AND MANAGEMENT.** System events are monitored and analyzed in a timely manner in accordance with ServiceNow’s current standard operating procedures. Response teams will be escalated to and engaged as necessary to address a security incident.

5.2 **BREACH NOTIFICATION.**

5.2.1. **NOTIFICATION.** ServiceNow will report to Customer any accidental or unlawful destruction, loss, alteration, unauthorized disclosure, of or access to Customer Data ("Breach") without undue delay following determination by ServiceNow that a Breach has occurred.
5.2.2. **REPORT.** The initial report will be made to Customer’s security or privacy contact(s) designated in ServiceNow’s customer support portal (or if no such contact(s) are designated, to the primary technical contact designated by Customer). As relevant information in relation to the Breach is collected or otherwise becomes available to ServiceNow, it will provide such information without undue delay to Customer, to assist Customer to comply with its notification obligations under Data Protection Laws. In particular, to the extent reasonably possible and applicable, ServiceNow will provide Customer with the information described in Article 33 of GDPR.

5.2.3. **DATA CONTROLLER OBLIGATIONS.** Customer will cooperate with ServiceNow in maintaining accurate contact information in the customer support portal and by providing any information that is reasonably requested to resolve any security incident, including any Breaches, identify its root cause(s) and prevent a recurrence. Customer is solely responsible for determining whether to notify the relevant supervisory or regulatory authorities and impacted Data Subjects in relation to any Breach and for providing such notice.

6. **PENETRATION TESTS**

6.1 **BY A THIRD-PARTY.** For each family release, skilled third-party vendors will perform penetration testing on the applications on the ServiceNow platform to identify vulnerabilities. Executive reports from the penetration testing are made available to Customer in ServiceNow CORE.

6.2 **BY CUSTOMER.** Customer may request to perform, at its own expense, an application penetration test for applications in which Customer Data is stored; provided that Customer will: (i) notify ServiceNow and submit a request to schedule such a test using the Support Portal per ServiceNow’s then-current penetration testing policy, and (ii) agree to ServiceNow’s penetration test agreement prior to conducting such test. In the event Customer’s authorized penetration testing identifies vulnerabilities that ServiceNow is able to reproduce, ServiceNow will, consistent with industry-standard practices, use commercially reasonable efforts to promptly make any necessary changes to improve the security of the Subscription Service.

7. **SHARED SECURITY RESPONSIBILITY**

7.1 **PRODUCT CAPABILITIES.** ServiceNow provides a variety of security settings that allow Customer to configure security of the Subscription Services for their own use such as, but not limited to: (i) authenticate users before accessing the Customer’s instance; (ii) encrypt passwords; (iii) allow users to manage passwords; and (iv) access instance application logs. Customer will manage each user’s access to and use of the Subscription Services by assigning to each user a credential and user type that controls the level of access to the applicable Subscription Services. Customer bears sole responsibility for reviewing the Security Program and making an independent determination as to whether it meets Customer’s requirements, taking into account the type and sensitivity of Customer Data that Customer provides to ServiceNow. Customer bears sole responsibility for implementing encryption and access control functionalities within the instance to protect Customer Data and assumes all liability for damages directly resulting from any decision not to encrypt Customer Data. Customer bears sole responsibility for protecting the confidentiality of each user’s login and password and managing each user’s access to the Subscription Services. Customer will be solely responsible for implementing the documented best practices and hardening guidelines for securing its ServiceNow instances.

7.2 **SECURITY CONTACT.** In accordance with the Customer Support Policy (www.servicenow.com/upgrade-schedules.html), Customer agrees to identify and maintain appropriate security contact(s) for all information security incident and information security-related communication within the Support Portal.

7.3 **LIMITATIONS.** Notwithstanding anything to the contrary in this DSA or other parts of the Agreement, ServiceNow’s obligations herein are only applicable to the Subscription Services. This DSA does not apply to: (i) information shared with ServiceNow that is not Customer Data; (ii) data in Customer’s VPN or a third-party network; and (iii) any data processed by Customer or its users in violation of the Agreement or this DSA.