servicenow

SERVICENOW NATIONAL SECURITY CLOUD ADDENDUM

This Service Now National Security Cloud addendum ("**NSC Addendum**") sets forth the modified or supplemental terms applicable to ServiceNow's operation and Customer's use of the ServiceNow Subscription Services that are hosted in ServiceNow's National Security Cloud ("**NSC**") environment ("**NSC Hosted Products**"). To the extent there is any conflict between the ServiceNow Public Sector Subscription Terms of Service ("**Terms of Service**") and the terms of this NSC Addendum, the terms of this NSC Addendum shall prevail with respect to NSC Hosted Products. All capitalized terms not defined in this NSC Addendum have the meaning given to them in the Terms of Service. For the avoidance of doubt, this NSC Addendum shall not apply to the services or products hosted in environments other than the NSC, professional services, or applications from the ServiceNow Store.

1. **Support**. Customer Support for the NSC Hosted Products will be provided by ServiceNow's technical support team located in the U.S., by personnel who are U.S. citizens or permanent residents with at least three years of residency in the U.S.

2. **Pre-approved Sub-Processors**. Notwithstanding anything to the contrary in the DPA or any other data processing agreement between Customer and ServiceNow, ServiceNow, Inc. and Microsoft Corporation (and any further sub-processors appointed by Microsoft) are added to the list of pre-approved sub-processors between ServiceNow and Customer for the NSC Hosted Products.

3. **Data Security Addendum**. This Section 3 modifies or supplements the DSA for the NSC Hosted Products:

a. **Security Program.** All references to ISO27001, ISO27018, SSAE 18 / SOC 1 and SOC 2 Type 2 in Section 1 (Security Program) of the DSA shall be replaced with NIST Special Publication 800-53, or substantially equivalent standards, governing the processing, storage, transmission, and security of Customer Data.

b. **Certifications and Attestations.** Section 2.1 of the DSA (Certifications and Attestations) is deleted in its entirety and replaced with the following: "**DEPARTMENT OF DEFENSE (DOD) IMPACT LEVEL 5 (IL5) AUTHORIZATION.** ServiceNow shall establish and maintain an IL5 Authorization for the Security Program supporting the Subscription Service. At least once per calendar year, ServiceNow shall undergo an annual assessment by a Third-Party Assessment Organization ("**3PAO**"), as required to maintain IL5 Authorization."

c. **Audit.** The following shall be added to Section 2.2 (Audit) of the DSA: "Service Now shall make the report resulting from the 3PAO annual assessment available to Customer in ServiceNow CORE or an alternative documentation portal."

d. **Vulnerability Management.** In Section 3.2.4 of the DSA (Vulnerability Management), "at least quarterly" is deleted and replaced with "at least monthly."

e. **Data Encryption At Rest.**

i. Section 3.2.9 (Data Encryption at Rest) of the DSA is deleted in its entirety and replaced with the following: "ServiceNow will encrypt Customer Data at-rest in accordance with the System Security Plan. Customer, at their own discretion, may additionally enable encryption features made available within the NSC Hosted Products."

ii. The fourth sentence of Section 7.1 (Product Capabilities) of the DSA is deleted in its entirety and replaced with the following: "Customer bears sole responsibility for implementing optional or customer-controlled encryption and access control

functionalities within Customer's instance to protect Customer Data and assumes all liability for damages directly resulting from any decision not to enable customer-controlled encryption of Customer Data."

f. **Data Location**. Section 4.1 (Data Location) of the DSA shall be deleted in its entirety and replaced with: "ServiceNow will host the purchased instances in data centers located in the United States which have attained IL5 Authorization."

g. **ServiceNow CORE**. References to "ServiceNow CORE" shall be deleted and replaced with "ServiceNow CORE or alternative documentation portal."

4. **Evaluation of Use Case.** ServiceNow's NSC operating environment is authorized at the level specified in the ServiceNow Ordering Documents. Customers are responsible for analyzing whether the authorized level and connection type is appropriate for the Customer's use case and Customer Data types. Certain products may be made available in NSC after the necessary independent audit (e.g., 3PAO) is complete and the products are formally recommended for approval, but the AO has not yet approved the request. ServiceNow will use reasonable efforts to publish and maintain a list of products that are available under these conditions. Moreover, ServiceNow and other third-party Applications (Apps) provided via the ServiceNow App Store or other means may not be within scope of ServiceNow's P-ATOs. Customer is required to determine whether the product(s) meets their security requirements prior to installation and usage.

5. **Customer Monitoring Rights**. All references in the DPA regarding Customer's ability to audit ServiceNow's policies and procedures governing the security of Customer Data shall be replaced with the following: "Data Processor shall enable Customer to conduct an audit of ServiceNow in accordance with Section 2 of the DSA."

///
///
///

Remainder of page intentionally left blank