SUBSCRIPTION SERVICE GUIDE

1. DEFINITIONS

1.1. "**Available**" means that the Subscription Service can be accessed by authorized users.

1.2. "*Excused Downtime*" means: (i) Maintenance Time of up to two (2) hours per month; and (ii) any time the Subscription Service is not Available due to circumstances beyond ServiceNow's control, including without limitation modifications of the Subscription Service by any person other than ServiceNow or a person acting at ServiceNow's direction, a Force Majeure Event, general Internet outages, failure of Customer's infrastructure or connectivity (including without limitation, direct connectivity and virtual private network (VPN) connectivity to the Subscription Service), computer and telecommunications failures and delays, and network intrusions or denial-of-service or other criminal attacks.

1.3. "*Infrastructure Maintenance*" means any repairs, maintenance or improvements to the cloud infrastructure used by ServiceNow to operate and deliver the Subscription Service. ServiceNow will give Customer ten (10) days prior notice of Infrastructure Maintenance if ServiceNow in its reasonable judgment believes that any Infrastructure Maintenance will impact Customer's use of its production instances of the Subscription Service, unless the Infrastructure Maintenance is essential to the security or operation of the Subscription Service.

1.4. "*Maintenance Time*" means the time the Subscription Service is not Available due to Infrastructure Maintenance, Upgrades and Updates.

1.5. "*Availability SLA*" means that the production instances of the Subscription Service will be Available at least ninety-nine and eight-tenths percent (99.8%) of the time during a calendar month, excluding Excused Downtime.

2. SUPPORT

During the Subscription Term, ServiceNow shall provide support for the Subscription Service as set forth in the *Customer Support Policy* attached hereto, and incorporated herein by reference. The Customer Support Policy may be updated from time to time.

3. UPGRADES

ServiceNow determines whether and when to develop, release and apply any Upgrade or Update (as defined in the *Upgrade and Update Policy* attached hereto, and incorporated herein by reference) to Customer's instances of the Subscription Service in accordance with the Upgrade and Update Policy. The Upgrade and Update Policy may be updated from time to time.

4. DATA SECURITY

ServiceNow shall implement and maintain security procedures and practices appropriate to information technology service providers to protect Customer Data from unauthorized access, destruction, use, modification, or disclosure, as described in the *Data Processing Annex* and the *Data Security Guide* attached hereto, and incorporated herein by reference.

5. AVAILABILITY SERVICE LEVEL

5.1. AVAILABILITY. If Customer's production instances of the Subscription Service fall below the Availability SLA, Customer's exclusive remedy for failure of the Subscription Service to meet the Availability SLAs is either: (a) to request that the affected Subscription Term be extended for the number of minutes the Subscription Service was not Available in the month in accordance with the Availability SLA; or (b) to request that ServiceNow issue a service credit to Customer for the dollar value of the number of minutes the Subscription Service was not Available in the month in accordance with the Availability SLA (determined at the deemed per minute rate ServiceNow charges to Customer for Customer's use of the affected Subscription Service), which Customer may request ServiceNow apply to the next invoice for subscription fees.

5.2. REQUESTS. Customer must request all service credits or extensions in writing to ServiceNow within thirty (30) days of the end of the month in which the Availability SLA was not met, identifying the support requests relating to the period Customer's production instances of the Subscription Service was not Available. The

total amount of service credits for any month may not exceed the subscription fee for the affected Subscription Service for the month, and has no cash value. ServiceNow may delay issuing service credits until such amounts reach one thousand U.S. dollars ($1,000) or equivalent currency specified in the applicable Order Form.

6.   INSURANCE

ServiceNow agrees to maintain in effect during the Subscription Term, at ServiceNow's expense, the following minimum insurance coverage:

(a)   Workers' Compensation Insurance, in accordance with applicable statutory, federal, and other legal requirements and Employers' Liability Insurance covering ServiceNow's employees in an amount of not less than $1,000,000 for bodily injury by accident, $1,000,000 policy limit for bodily injury by disease, and $1,000,000 each employee for bodily injury by disease;

(b)   Commercial General Liability Insurance written on an occurrence form and including coverage for bodily injury, property damage, products and completed operations, personal injury, advertising injury arising out of the services and/or products provided by ServiceNow under this Agreement with minimum limits of $1,000,000 per occurrence/$2,000,000 aggregate;

(c)   Commercial Automobile Liability Insurance providing coverage for hired and non-owned automobiles used in connection with this Agreement in an amount of not less than $1,000,000 per accident combined single limit for bodily injury and property damage;

(d)   Combined Technology Errors & Omission Policy with a $5,000,000 per claim limit, including: (i) Professional Liability Insurance providing coverage for the services and software in this Agreement. Such coverage to be maintained for at least two (2) years after the termination of this Agreement; and (ii) Privacy, Security, and Media Liability Insurance providing liability coverage for unauthorized access or disclosure, security breaches or system attacks, as well as infringements of copyright and trademark that might result from this Agreement; and

(e)   Excess Liability over Employers' Liability, Commercial General Liability and Commercial Automobile Liability with a $5,000,000 aggregate limit.

For the purpose of this Section 6, a "*claim*" means a written demand for money or a civil proceeding which is commenced by service of a complaint or similar pleading.

CUSTOMER SUPPORT POLICY

This Customer Support Policy governs the support that ServiceNow will provide for its Subscription Service ("***Customer Support***").

1. SCOPE

The purpose of Customer Support is to resolve defects that cause the Subscription Service to perform not in substantial conformance to the Product Overview. A resolution to a defect may consist of a fix, workaround or other relief ServiceNow deems reasonable.

Customer Support does not include performing the following services:

- implementation services
- configuration services
- integration services
- customization services or other custom software development
- training
- assistance with administrative functions

Customer Support is not required to provide resolutions for immaterial defects or defects due to modifications of the Subscription Service made by any person other than ServiceNow or a person acting at ServiceNow's direction.

2. BUSINESS HOURS

Customer Support is available 24 hours a day, 7 days a week, including all holidays.

3. ACCESS CONTACTS

- Support Portal at https://hi.service-now.com/. Customer may get login access to this self-service portal by contacting its ServiceNow administrator.
- Phone using one of the numbers at http://servicenow.com/support/contact-support.html.

4. INCIDENT PRIORITY

Incident priority for a defect is determined using the guidelines below:

Priority	Definition
P1	Any defect that causes an instance not to be Available
P2	Any defect that causes a critical function to fail
P3	Any defect that significantly impedes work or progress
P4	Any defect that does not significantly impede work or progress

5. RESPONSE TIME AND LEVEL OF EFFORT

Customer may submit an incident with ServiceNow via phone or web. All support requests are tracked online and can be viewed by Customer's authorized contacts. Response times do not vary if the incident was filed via phone or web.

ServiceNow will use reasonable efforts to meet the target response times and target level of effort stated in the table below:

Priority	Target Response Times	Target Level of Effort
P1	30 minutes	Continuously, 24 hours per day, 7 days per week
P2	2 hours	Continuously, but not necessarily 24 hours per day, 7 days per week
P3	1 business day	As appropriate during normal business hours
P4	NA	Varies

6. CUSTOMER RESPONSIBILITIES

Customer's obligations are as follows:

(a) Customer agrees to receive from ServiceNow communications via email, phone or through the Support Portal regarding the Subscription Service.

(b) Customer shall appoint no more than ten (10) contacts ("***Customer Authorized Contacts***") to engage Customer Support for questions and/or technical issues.

(c) Customer must maintain the following Customer Authorized Contacts:

- Primary Business Contact
- Secondary Business Contact
- Technical Contact
- Support Contact
- Primary Customer Administrator
- Security Contact

(d) Customer must ensure the information for all Customer Authorized Contacts is current in the Support Portal at https://hi.service-now.com/.

(e) Only Customer Authorized Contacts are authorized to contact Customer Support.

(f) Customer Authorized Contacts must be trained on the use and administration of the Subscription Service.

Customer shall cooperate to enable ServiceNow to deliver the Subscription Service and support for the Subscription Service. Customer is solely responsible for the use of the Subscription Service by its authorized users.

UPGRADE AND UPDATE POLICY

1. DEFINITIONS

1.1. "*Upgrades*" are ServiceNow's releases of the Subscription Service for enhancements or new features (including a new Release Family) applied by ServiceNow to Customer's instances of the Subscription Service at no additional fee during the Subscription Term.

1.2. "*Updates*" are ServiceNow's releases (including patches and hotfixes) of the Subscription Service applied by ServiceNow to Customer's instances of the Subscription Service at no additional fee during the Subscription Term that provide problem fixes, but do not generally include new functionality, and are released as needed.

1.3. "*Release Family*" is an Upgrade that is a complete solution with new features or enhancements, including previously released Updates if applicable to the features included in the Upgrade. For example, ServiceNow's "Geneva" Upgrade established the "Geneva Release Family", and ServiceNow's "Helsinki" Upgrade established the "Helsinki Release Family".

1.4. "*Critical Upgrade*" is an Upgrade that in ServiceNow's reasonable judgment is critical to maintaining the availability, security or performance of the Subscription Service; comply with applicable laws or to avoid infringement or misappropriation of a third-party Intellectual Property Right.

1.5. "*Critical Update*" is an Update that in ServiceNow's reasonable judgment is critical to maintaining the availability, security or performance of the Subscription Service; comply with applicable laws or to avoid infringement or misappropriation of a third-party Intellectual Property Right.

1.6. "*Supported Release Family*" at a particular time means the then-current Release Family and the prior two (2) Release Families.

2. UPGRADES AND UPDATES

ServiceNow shall determine, in its sole discretion: (a) whether and when to develop, release and apply any Update or Upgrade to Customer's instances of the Subscription Service; and (b) whether a particular release is an Update, Upgrade or new service offering that is available separately for purchase.

3. NOTICE

ServiceNow shall: (a) give Customer thirty (30) days' notice of any Upgrade to the Subscription Service; and (b) use reasonable efforts to give Customer ten (10) days' notice of any Update to the Subscription Service. Notwithstanding the foregoing, ServiceNow may provide Customer with shorter notice or no notice before the application of a Critical Upgrade or a Critical Update.

4. SUPPORTED AND NON-SUPPORTED RELEASE FAMILIES

Customer acknowledges that the current Release Family is the version of the Subscription Service containing the most current features, availability, performance and security. Within a Supported Release Family, the most recent Update is the version of the Subscription Service for that Release Family that contains the most current problem fixes, availability, performance and security. A Customer using a Supported Release Family may be required to apply a Critical Update within the Supported Release Family. A Customer that has not Upgraded to a Supported Release Family may experience defects, for which Customer hereby agrees that ServiceNow is not responsible, including without limitation those that affect the features, availability, performance and security of the Subscription Service, that are fixed in the most current version of the Subscription Service. A Customer who is not using a Supported Release Family may be required to apply an Upgrade to a Supported Release Family.

DATA PROCESSING ANNEX

This Data Processing Annex ("**DPA**") forms a part of the Agreement and reflects the parties' agreement with respect to the Processing of Personal Data submitted to the Subscription Service by Customer.

In the event of any conflict between the terms of this DPA and the terms of the Agreement with respect to the subject matter herein, this DPA shall control. All capitalized terms not defined in this DPA will have the meaning given to them in other parts of the Agreement.

1. DEFINITIONS

1.1. "**Data Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of Processing of Personal Data. For purposes of this DPA, Data Controller is Customer and, where applicable, its Affiliates either permitted by Customer to submit Personal Data to the Subscription Service or whose Personal Data is Processed in the Subscription Service.

1.2. "**Data Processor**" means the natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Data Controller. For purposes of this DPA, Data Processor is the ServiceNow entity that is a party to the Agreement.

1.3. "**Data Protection Laws**" means all applicable laws and regulations regarding the Processing of Personal Data.

1.4. "**Data Subject**" means an identified or identifiable natural person.

1.5. "**Personal Data**" means any information relating to a Data Subject uploaded by or for Customer or Customer's agents, employees, or contractors to the Subscription Service as Customer Data.

1.6. "**Process**" or "**Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.7. "**Sub-Processor**" means any legal person or entity engaged in the Processing of Personal Data by Data Processor. For the avoidance of doubt, ServiceNow's colocation datacenter facilities are not Sub-Processors under this DPA.

2. SCOPE OF THE PROCESSING

2.1. <u>COMMISSIONED PROCESSOR</u>. Data Controller appoints Data Processor to Process Personal Data on behalf of Data Controller to the extent necessary to provide the Subscription Service described in the Agreement and in accordance with the Instructions (as defined below).

2.2. <u>INSTRUCTIONS</u>. The Agreement constitutes Data Controller's written instructions to Data Processor for Processing of Personal Data. Data Controller may issue additional or alternate data processing instructions provided that such instructions are: (a) consistent with the purpose and the scope of the Agreement; and (b) confirmed in writing by Data Controller. For the avoidance of doubt, Data Controller shall not use additional or alternate instructions to alter the scope of the Agreement. For the purposes of this Agreement, the term "Instructions" means Data Controller's documented data processing instructions issued to Data Processor in compliance with this Section 2. Data Controller is responsible for ensuring its Instructions to Data Processor comply with Data Protection Laws.

2.3. <u>NATURE, SCOPE AND PURPOSE OF THE PROCESSING</u>. Data Processor shall only Process Personal Data in accordance with Data Controller's Instructions and to the extent necessary for providing the Subscription Service as described in the Agreement.

2.4. <u>CATEGORIES OF PERSONAL DATA AND CATEGORIES OF DATA SUBJECTS</u>. Data Controller may submit Personal Data to the Subscription Service as Customer Data, the extent of which is determined and controlled by Data Controller in its sole discretion and is further described in Appendix 1.

3. DATA CONTROLLER

3.1. COMPLIANCE WITH DATA PROTECTION LAWS. Data Controller shall comply with all of its obligations under Data Protection Laws when Processing Personal Data.

3.2. SECURITY RISK ASSESSMENT. Data Controller agrees that in accordance with Data Protection Laws and before submitting any Personal Data to the Subscription Service, Data Controller will perform an appropriate risk assessment to determine whether the security measures within the Subscription Service provide an adequate level of security, taking into account the nature, scope, context and purposes of the processing, the risks associated with the Personal Data and the applicable Data Protection Laws. Data Controller is solely responsible for determining the adequacy of the security measures within the Subscription Service in relation to the Personal Data Processed. As further described in Section 7.1 (Product Capabilities) of the Data Security Guide, the Subscription Service includes, without limitation, column level encryption functionality and role-based access control, which Data Controller may use in its sole discretion to ensure a level of security appropriate to the risk of the Personal Data. For clarity, Data Controller may influence the scope and the manner of Processing of its Personal Data by its own implementation, configuration (i.e., different types of encryption) and use of the Subscription Service, including any other products or services offered by ServiceNow and third-party integrations.

3.3. CUSTOMER'S AFFILIATES. The obligations of Data Processor set forth herein will extend to Customer's Data Controller Affiliates to which Customer provides access to the Subscription Service or whose Personal Data is Processed within the Subscription Service, subject to the following conditions:

3.3.1. Compliance. Customer shall at all times be liable for its Affiliates' compliance with this DPA and all acts and omissions by a Data Controller Affiliate are considered acts and omissions of Customer; and

3.3.2. Claims. Customer's Data Controller Affiliates will not bring a claim directly against Data Processor. In the event a Data Controller Affiliate wishes to assert a valid legal action, suit, claim or proceeding against Data Processor (a "***Data Controller Affiliate Claim***"): (i) Customer must bring such Data Controller Affiliate Claim directly against Data Processor on behalf of such Data Controller Affiliate, unless Data Protection Laws require that Data Controller Affiliate be party to such Data Controller Affiliate Claim; and (ii) all Data Controller Affiliate Claims will be considered claims made by Customer and are at all times subject to any aggregate limitation of liability set forth in the Agreement.

3.4. COMMUNICATION. Unless otherwise provided in this DPA, all requests, notices, cooperation and communication, including Instructions issued or required under this DPA (collectively, "***Communication***"), must be in writing and between Customer and ServiceNow only and Customer shall inform the applicable Data Controller Affiliate of any Communication from ServiceNow pursuant to this DPA. Customer shall be solely responsible for ensuring that any Communications (including Instructions) it provides to ServiceNow relating to Personal Data for which a Customer Affiliate is Data Controller reflect the relevant Customer Affiliate's intentions.

4. DATA PROCESSOR

4.1. DATA CONTROLLER'S INSTRUCTIONS. Data Processor will have no liability for any harm or damages resulting from Data Processor's compliance with Instructions received from Data Controller. Where Data Processor believes that compliance with Data Controller's Instructions could result in a violation of Data Protection Laws or is not in the ordinary course of Data Processor's obligations in operating the Subscription Service, Data Processor shall promptly notify Data Controller thereof. Data Controller acknowledges that Data Processor is reliant on Data Controller's representations regarding the extent to which Data Controller is entitled to Process Personal Data.

4.2. DATA PROCESSOR PERSONNEL. Access to Personal Data by Data Processor will be limited to personnel who require such access to perform Data Processor's obligations under the Agreement and who are bound by obligations to maintain the confidentiality of such Personal Data.

4.3. DATA SECURITY MEASURES. Without prejudice to Data Controller's security risk assessment obligations under Section 3.2 (Security Risk Assessment) above, Data Processor shall maintain appropriate technical and organizational safeguards to protect the security, confidentiality and integrity of Customer Data, including any Personal Data contained therein, as described in Section 2 (Physical, Technical and Administrative

Security Measures) of the Data Security Guide. Such measures are designed to protect Customer Data from loss, alteration, unauthorized access, acquisition, use, disclosure, or accidental or unlawful destruction, and include:

4.3.1.   **Service Access Control.** The Subscription Service provides user and role based access controls. Data Controller is responsible for configuring such access controls within its instance.

4.3.2.   **Logging and Monitoring.** The production infrastructure log activities are centrally collected and are secured in an effort to prevent tampering and are monitored for anomalies by a trained security team.

4.3.3.   **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.

4.3.4.   **Service Continuity.** The production database servers are replicated in near real time to a mirrored data center in a different geographic region.

4.3.5.   **Testing.** Data Processor regularly tests, assess and evaluates the effectiveness of its information security program and may periodically review and update the such program to address new and evolving security technologies, changes to industry standard practices, and changing security threats.

4.4.   DELETION OF PERSONAL DATA. Upon termination or expiration of the Agreement, Data Processor shall return and delete Customer Data, including Personal Data contained therein, as described in the Agreement.

4.5.   DATA CENTERS. Data Processor will host Data Controller's instances of the Subscription Service in data centers located in the geographic regions specified on the Order Form.

5.   REQUESTS MADE FROM DATA SUBJECTS AND AUTHORITIES

5.1.   REQUESTS FROM DATA SUBJECTS. During the Subscription Term, Data Processor shall provide Data Controller with the ability to access, correct, rectify, erase or block Personal Data, or to transfer or port such Personal Data, within the Subscription Service, as may be required under Data Protection Laws (collectively, "*Data Subject Requests*").

5.2.   RESPONSES. Data Controller will be solely responsible for responding to any Data Subject Requests, provided that Data Processor shall reasonably cooperate with the Data Controller to respond to Data Subject Requests to the extent Data Controller is unable to fulfill such Data Subject Requests using the functionality in the Subscription Service. Data Processor will instruct the Data Subject to contact the Customer in the event Data Processor receives a Data Subject Request directly.

5.3.   REQUESTS FROM AUTHORITIES. In the case of a notice, audit, inquiry or investigation by a government body, data protection authority or law enforcement agency regarding the Processing of Personal Data, Data Processor shall promptly notify Data Controller unless prohibited by applicable law. Data Controller shall keep records of the Personal Data Processed by Data Processor, and shall cooperate and provide all necessary information to Data Processor in the event Data Processor is required to produce such information to a data protection authority.

5.4.   COSTS. Customer shall reimburse ServiceNow for any reasonable additional costs incurred in connection with the fulfilment of ServiceNow's obligations under Sections 5.2. and 5.3. above.

6.   BREACH NOTIFICATION

Data Processor shall report to Data Controller any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Data that it becomes aware of without undue delay.

7.   CUSTOMER MONITORING RIGHTS

Customer may audit Data Processor's Processing of Personal Data under this DPA by exercising its audit rights set forth in Section 4.2 (Audits and Corrective Actions) of the Data Security Guide.

8. SUB-PROCESSORS

8.1. <u>USE OF SUB-PROCESSORS</u>. Data Controller authorizes Data Processor to engage Sub-Processors appointed in accordance with this Section 8 to support the provision of the Subscription Service and to deliver Professional Services as described in the Agreement.

8.1.1. ServiceNow Affiliates. As of the Effective Date, Data Processor engages, as applicable, the following ServiceNow Affiliates as Sub-Processors: ServiceNow, Inc. (USA), ServiceNow Nederland B.V. (the Netherlands), ServiceNow Australia Pty Ltd (Australia), ServiceNow Software Development India Private Limited (India) and ServiceNow UK Ltd. (United Kingdom) (collectively, "***Sub-Processor Affiliates***"). Data Processor will notify Data Controller of changes regarding such Sub-Processor Affiliates through Data Processor's customer support portal (or other mechanism used to notify its general customer base). Each Sub-Processor Affiliate shall comply with the obligations of the Agreement in the Processing of the Personal Data.

8.1.2. New Sub-Processors. Prior to Data Processor or a Data Processor Affiliate engaging a Sub-Processor, Data Processor shall: (i) notify Data Controller by email to Customer's designated contact(s) or by notification within the customer support portal (or other mechanism used to notify its customer base); and (ii) ensure that such Sub-Processor has entered into a written agreement with Data Processor (or the relevant Data Processor Affiliate) requiring that the Sub-Processor abide by terms no less protective than those provided in this DPA. Upon written request by Data Controller, Data Processor shall make a summary of the data processing terms available to Data Controller. Data Controller may request in writing reasonable additional information with respect to Sub-Processor's ability to perform the relevant Processing activities in accordance with this DPA.

8.2. <u>RIGHT TO OBJECT</u>. Data Controller may object to Data Processor's proposed use of a new Sub-Processor by notifying Data Processor within ten (10) days after receipt of Data Processor's notice if Data Controller reasonably determines that such Sub-Processor is unable to Process Personal Data in accordance with the terms of this DPA ("***Controller Objection Notice***"). Data Processor shall notify Data Controller within thirty (30) days from receipt of the Controller Objection Notice if Data Processor intends to provide the applicable Professional Service or Subscription Service with the use of the Sub-Processor at issue, and Customer may terminate the applicable Order Form(s) with respect to the Professional Service or Subscription Service that require use of the Sub-Processor at issue upon written notice to ServiceNow within forty-five (45) days of the date of Controller Objection Notice and, as Customer's sole and exclusive remedy, ServiceNow will refund to Customer any unused prepaid fees.

8.3. <u>LIABILITY</u>. Use of a Sub-Processor will not relieve, waive or diminish any obligation Data Processor has under the Agreement, and Data Processor is liable for the acts and omissions of any Sub-Processor to the same extent as if the acts or omissions were performed by Data Processor.

9. INTERNATIONAL DATA TRANSFERS

9.1. <u>STANDARD CONTRACTUAL CLAUSES AND ADEQUACY</u>. Where required under Data Protection Laws, Data Processor or Data Processor's Affiliates shall require Sub-Processors to abide by (i) the Standard Contractual Clauses for Data Processors established in third countries; or (ii) another lawful mechanism for the transfer of Personal Data as approved by the European Commission.

9.2. <u>PRIVACY SHIELD</u>. ServiceNow, Inc. shall comply with the EU-U.S. and Swiss-U.S. Privacy Shield Framework set forth by the United States Department of Commerce with respect to the Processing of Personal Data transferred from the European Economic Area and Switzerland to the United States.

10. DATA PROTECTION IMPACT ASSESSMENTS

Effective May 25, 2018, Data Processor will, on request, provide Data Controller with reasonable information required to fulfill Data Controller's obligations under the General Data Protection Regulation (2016/679) ("***GDPR***") to carry out data protection impact assessments, if any, for Processing of Personal Data within the Subscription Service. Data Controller is solely responsible for any prior consultation with a supervisory authority required for Processing of Personal Data under GDPR.

APPENDIX 1

DETAILS OF PROCESSING

Nature and Purpose of Processing

Data Processor will Process Personal Data as required to provide the Subscription Service and in accordance with the Agreement.

Duration of Processing

Data Processor will Process Personal Data for the duration of the Agreement and in accordance with Section 4 (Data Processor) of this DPA.

Data Subjects

Data Controller may submit Personal Data to the Subscription Service, the extent of which is solely determined by Data Controller, and may include Personal Data relating to the following categories of Data Subjects:

- Clients and other business contacts;
- Employees and contractors;
- Subcontractors and agents; and
- Consultants and partners.

Categories of Personal Data

Data Controller may submit Personal Data to the Subscription Service, the extent of which is solely determined by Data Controller, and may include the following categories:

- communication data (e.g. telephone, email);
- business and personal contact details;
- and other Personal Data submitted to the Subscription Service.

Special Categories of Personal Data

Data Controller may submit Special Categories of Personal Data to the Subscription Service, the extent of which is solely determined by Data Controller in compliance with Data Protection Law, and may include the following categories, if any:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data or biometric data;
- health information; and
- sex life or sexual orientation.

Processing Operations

The personal data transferred will be subject to the following basic processing activities:

- All activities necessary for the performance of the Agreement.

DATA SECURITY GUIDE

This Data Security Guide describes the measures ServiceNow takes to protect Customer Data. This Data Security Guide forms a part of any legal agreement into which this Data Security Guide is explicitly incorporated by reference (the "***Agreement***") and is subject to the terms of the Agreement. Capitalized terms not otherwise defined in this Data Security Guide will have the meaning given to them in other parts of the Agreement.

1. SECURITY PROGRAM

While providing the Subscription Service, ServiceNow will maintain a written information security program of policies, procedures and controls governing the processing, storage, transmission and security of Customer Data (the "***Security Program***"). The Security Program includes industry-standard practices designed to protect Customer Data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access. ServiceNow regularly tests, assesses and evaluates the effectiveness of the Security Program and may periodically review and update the 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. (i) 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 (ii) fire detection and fire suppression systems both localized and throughout the data center floor.

2.1.2. Systems, Machines and Devices. (i) Physical protection mechanisms; and (ii) entry controls to limit physical access.

2.1.3. Media. (i) Industry standard destruction of sensitive materials before disposition of media; (ii) secure safe for storing damaged hard disks prior to physical destruction; and (iii) physical destruction of all decommissioned hard disks storing Customer Data.

2.2. TECHNICAL SECURITY MEASURES.

2.2.1. Access Administration. Access to the Subscription Service by ServiceNow employees and contractors is protected by authentication and authorization mechanisms. User authentication is required to gain access to production and sub-production instances. 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., the required use of VPN connections, complex passwords with expiration dates, and a two-factored authenticated connection) and is accessible for administration.

2.2.2. Service Access Control. The Subscription Service provides user and role based access controls. Customer is responsible for configuring such access controls within its instance.

2.2.3. Logging and Monitoring. The production infrastructure log activities are centrally collected and are secured in an effort to prevent tampering and are monitored for anomalies by a trained security team.

2.2.4. Firewall System. An industry-standard firewall is installed and managed to protect ServiceNow systems by residing on the network to inspect all ingress connections routed to the ServiceNow environment.

2.2.5. Vulnerability Management. ServiceNow conducts periodic independent security risk evaluations to identify critical information assets, assess threats to such assets, determine potential vulnerabilities, and provide for remediation. When software vulnerabilities are revealed and addressed by a vendor patch, ServiceNow will obtain the patch from the applicable vendor and apply it within an appropriate timeframe in accordance with ServiceNow's 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 all production systems.

2.2.6. Antivirus. ServiceNow updates antivirus, anti-malware, and anti-spyware software on regular intervals and centrally logs events for effectiveness of such software.

2.2.7. Change Control. ServiceNow ensures that changes to platform, applications and production infrastructure are evaluated to minimize risk and are implemented following ServiceNow's standard operating procedure.

2.2.8. 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. Data Center Inspections. ServiceNow performs routine reviews at each data center to ensure that it continues to maintain the security controls necessary to comply with the Security Program.

2.3.2. Personnel Security. ServiceNow performs background and drug 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 applicable law.

2.3.3. Security Awareness and Training. ServiceNow maintains a security awareness 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.

2.3.4. Vendor Risk Management. ServiceNow maintains a vendor risk management program that assesses all vendors that access, store, process or transmit Customer Data for appropriate security controls and business disciplines.

3. SERVICE CONTINUITY

3.1. DATA CENTERS; DATA BACKUP. ServiceNow will host Customer's instances of the Subscription Service in a pair of data centers that attained SSAE 18 Type 2 attestations or have ISO 27001 certifications (or equivalent attestations) acting in an active/active capacity in the geographic regions specified on the Order Form for the Subscription Term. 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. The production database servers are replicated in near real time to a mirrored data center in a different geographic region. Each Customer instance is supported by a network configuration with multiple connections to the Internet. ServiceNow backs up all Customer Data in accordance with ServiceNow's standard operating procedure.

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 a ServiceNow telephone support representative, geographically distributed to ensure business continuity for support operations.

4. CERTIFICATIONS AND AUDITS

4.1. CERTIFICATIONS AND ATTESTATIONS. ServiceNow shall establish and maintain sufficient controls to meet the objectives stated in ISO 27001, ISO 27018, SSAE 18 / SOC 1 and SOC 2 Type 2 (or equivalent standards) (collectively, the "*Standards*") for the information security management system supporting the Subscription Service. At least once per calendar year, ServiceNow shall obtain an assessment against such Standards by an independent third-party auditor.

4.2. AUDITS AND CORRECTIVE ACTIONS.

4.2.1. Audits. Upon Customer's request, ServiceNow shall grant Customer access to the ServiceNow self-access documentation portal ("*ServiceNow CORE*"), where Customer may access industry-recognized documentation evidencing the Security Program ("*Audit*"). Such Audit will include a copy of ServiceNow's certification or audit reports performed by an independent third-party of ServiceNow's information security management system supporting the Subscription Service against the Standards.

4.2.2. Corrective Actions. ServiceNow and Customer may schedule a mutually convenient time to discuss the Audit. If a material deficiency is discovered between ServiceNow's commitments in this Data Security Guide and the information gathered during an Audit, then ServiceNow shall take, at its own cost, the necessary corrective actions. This sets forth Customer's exclusive rights and remedies (and ServiceNow's sole liability) with respect to any material deficiencies noted during an Audit. The Audit and the results derived therefrom are Confidential Information of ServiceNow.

5. MONITORING AND INCIDENT MANAGEMENT

5.1. MONITORING, MANAGEMENT AND NOTIFICATION.

5.1.1. Incident Monitoring and Management. ServiceNow will monitor, analyze and respond to security incidents in a timely manner in accordance with ServiceNow's standard operating procedure. ServiceNow's security group will escalate and engage response teams as may be necessary to address an incident.

5.1.2. Breach Notification. Unless notification is delayed by the actions or demands of a law enforcement agency, ServiceNow will report to Customer any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data (a "***Breach***") without undue delay following determination by ServiceNow that a Breach has occurred.

5.1.3. Report. The initial report will be made to Customer security or privacy contact(s) designated in ServiceNow's customer support portal (or if no such contact(s) are designated, to the primary contact designated by Customer). As information is collected or otherwise becomes available to ServiceNow, and unless prohibited by applicable law, ServiceNow shall provide without undue delay any further information regarding the nature and consequences of the Breach to allow Customer to notify relevant parties, including affected Data Subjects, government agencies and data protection authorities in accordance with Data Protection Laws. The report will include the name and contact information of the ServiceNow contact from whom additional information may be obtained. ServiceNow shall inform Customer of the measures that it will adopt to mitigate the cause of the Breach and to prevent future Breaches.

5.1.4. Customer 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 and for providing such notice.

5.2. USE OF AGGREGATE DATA. ServiceNow may collect, use and disclose quantitative data derived from Customer's use of the Subscription Service for industry analysis, benchmarking, analytics, marketing, and other business purposes in support of the provision of the Subscription Service. Any such data will be in aggregate form only and will not contain Customer Data.

5.3. COOKIES. When providing the Subscription Service, ServiceNow uses cookies to: (i) track session state; (ii) route a browser request to a specific node when multiple nodes are assigned; and (iii) recognize a user upon returning to the Subscription Service. Customer shall be responsible for providing notice to, and collecting any necessary consents from, its authorized users of the Subscription Service for ServiceNow's use of cookies.

6. PENETRATION TESTS

6.1. BY A THIRD-PARTY. ServiceNow contracts with third-party vendors to perform a penetration test on the ServiceNow application per family release to identify risks and remediation that help increase security.

6.2. BY CUSTOMER. No more than once per calendar year Customer may request to perform, at its own expense, an application penetration test of a sub-production instance of the Subscription Service. Customer shall notify ServiceNow in advance of any test by submitting a request to schedule an application penetration test using ServiceNow's customer support portal per ServiceNow's then-current penetration testing policy and procedure, including entering into ServiceNow's penetration test agreement. ServiceNow and Customer must agree on a mutually acceptable time for the test; and Customer shall not perform a penetration test without ServiceNow's express written authorization. The test must be of reasonable duration, but in no event longer than fourteen (14) days, and must not interfere with ServiceNow's day-to-day operations. Promptly on completion of the penetration

test, Customer shall provide ServiceNow with the test results including any detected vulnerability. Upon such notice, ServiceNow shall, consistent with industry-standard practices, use all commercially reasonable efforts to promptly make any necessary changes to improve the security of the Subscription Service. Customer shall treat the test results as Confidential Information of ServiceNow subject to the confidentiality and non-use requirements of the Agreement.

7.   SHARING THE SECURITY RESPONSIBILITY

7.1.   PRODUCT CAPABILITIES. The Subscription Service has the capabilities to: (i) authenticate users before access; (ii) encrypt passwords; (iii) allow users to manage passwords; and (iv) prevent access by users with an inactive account. Customer manages each user's access to and use of the Subscription Service by assigning to each user a credential and user type that controls the level of access to the Subscription Service. Customer shall be responsible for implementing encryption and access control functionalities available within the Subscription Service for protecting all Customer Data containing sensitive data, including credit card numbers, social security and other government-issued identification numbers, financial and health information, Personal Data, and any Personal Data deemed sensitive or "special categories of personal data" under Data Protection Laws. Customer is solely responsible for its decision not to encrypt such data and ServiceNow will have no liability to the extent that damages would have been mitigated by Customer's use of such encryption measures. Customer is responsible for protecting the confidentiality of each user's login and password and managing each user's access to the Subscription Service.

7.2.   CUSTOMER COOPERATION. Customer shall promptly apply any application upgrade that ServiceNow determines is necessary to maintain the security, performance or availability of the Subscription Service.

7.3.   LIMITATIONS. Notwithstanding anything to the contrary in this Data Security Guide or other parts of the Agreement, ServiceNow's obligations extend only to those systems, networks, network devices, facilities and components over which ServiceNow exercises control. This Data Security Guide does not apply to: (i) information shared with ServiceNow that is not data stored in its systems using the Subscription Service; (ii) data in Customer's VPN or a third-party network; (iii) any data processed by Customer or its users in violation of the Agreement or this Data Security Guide; or (iv) Integrated Products. For the purposes of this Data Security Guide, "***Integrated Products***" shall mean ServiceNow-provided integrations to third-party products or any other third-party products that are used by Customer in connection with the Subscription Service. Customer agrees that its use of such Integrated Products will be: (a) in compliance with all applicable laws, including but not limited to, Data Protection Laws; and (b) in accordance with its contractual agreement with the provider of such Integrated Products. Any Personal Data populated from the Integrated Products to the Subscription Service must be collected, used, disclosed and, if applicable, internationally transferred in accordance with Customer's privacy policy, which will adhere to Data Protection Laws. For clarity, as between ServiceNow and Customer, Customer assumes all liability for any breaches of confidentiality that occur outside of the Subscription Service.