UPGRADE POLICY

1. UPGRADES

"Upgrades" are ServiceNow's releases of the Subscription Service for repairs, enhancements, or new features applied by CDI to Customer's instances of the Subscription Services at no additional; fee during the Subscription Term. ServiceNow has the discretion to provide new functionality as an Upgrade or as different software or service for a separate fee. ServiceNow determines whether and when to develop, release and apply any Upgrade to Customer's instances of the Subscription Services.

2. NOTICE: MAINTENANCE DOWNTIME

CDI shall use reasonable efforts to give Customer thirty (30) days prior notice of any Upgrade to the Subscription Service. CDI shall use reasonable efforts to give Customer ten (10) days prior notice of any Upgrade to the cloud infrastructure network, hardware, or software used by CDI to operate and deliver the Subscription Service if CDI in its judgement believes the infrastructure Upgrade will impact Customer's use of its production instances of the Subscription Service. CDI will use commercially reasonable efforts to limit the period of time during which the Subscription Service is unavailable due to the application of Upgrades to no more than two (2) hours per month. Notwithstanding the foregoing, reasonable judgment of CDI, to maintain the availability, security, or performance of the Subscription Service or the ability of CDI of efficiently provide the Subscription Service.

3. NOMENCLATURE

A pending Upgrade may be a "Feature Release", "Patch" or "Hotfix". A "**Feature Release**" is an Upgrade that includes new features or enhancements. A "**Patch**" or a "**Hotfix**" is an Upgrade to a Feature Release that maintains the functionality of the Feature Release and does not include new functionality. ServiceNow refers to each Feature Release and it's associated Patches and Hotfixes as a "**Release Family**" For example ServiceNow's Feature Release "Aspen" established the "Aspen" Release Family, and ServicesNow's subsequent Feature Release "Berlin: established the "Berlin Release Family.

4. PINNING REQUESTS

Customers may submit a support request for "no Upgrade" not fewer than five (5) business days' prior to a pending Upgrade to Subscription Service. Subject to the terms and conditions of this Upgrade Policy, Customer's "no Upgrade" request shall be granted, and the Upgrade shall not be applied to Customer's instances of the Subscription Service.

5. SUPPORT AND NON-SUPPORTED RELEASE FAMILIES

ServiceNow/CDI offers support for the then current Release Family and the prior two (2) Release Families ("**Supported Release Families**") as set forth in the Customer Support Policy. A Customer using a Supported Release Family may be required to Upgrade to a Patch or Hotfix within the Supported Release Family to correct a defect. At its discretion, ServiceNow/CDI may offer limited support for additional Release Families ("**Non-Supported Release Families**") Without limiting ServiceNow/CDI's discretion to determine the availability of support for Non-Supported Release Families, a Customer using a Non-Supported Release Family may be required to Upgrade to recovery point objectives are not applicable to Non-Supported Release Families.

Customer acknowledges that the current Release Family is the most current feature, availability, performance, and security version of the Subscription Service. Within a Support Release Family, the most recent Patch contains the most current feature, availability, performance, and security version of the Subscription Service for that Release Family. A Customer that has submitted a "no Upgrade" request may experience defects, for which Customer hereby agrees the ServiceNow/CDI is not responsible, including without limitation those that affect the feature, availability, performance and security version of the Subscription Service, that is fixed in the most current version of the Subscription Service.

6. REQUIRED UPGRADES

If Customer has requested "no Upgrade" it may nevertheless be requried to Upgrade if in the reasonable judgement of

CDI the Upgrade is necessary to maintain the availability, security, or performance of the Subscription Service, as follows:

6.1 SUPPORTED RELEASE FAMILY. If Customer is using a Supported Release Family, it may be required to Upgrade to a Patch or Hotfix within the Supported Release Family.

6.2 NON-SUPPORTED RELEASE FAMILY. If Customer is using a Non-Supported Release Family, it may be required to Upgrade to a Supported Release Family.

7. EXCEPTIONS

Notwithstanding the other provisions of the Upgrade Policy, Customers may not submit a support request for "no Upgrade" for any Upgrade to, or this is essential for, the infrastructure network, hardware, or software used by CDI to operate and deliver the Subscription Service

DATA SECURITY GUIDE

Sercurity Statement of an Enterprise IT Cloud Company

The CDI cloud is built for the enterprise customer with every aspect aimed towards meeting the customer's demand for reliability, availability, and security. CDI's comprehensive approach to address this demand is enabling by the following: (a) CDI's robust cloud infrastructure runs on its own applications and utilizes industry best-of-breed technology to automate mission critical functionalities in the cloud service with around-the-clock and around-the-world delivery; (b) CDI achieves flexibility and control in its ability to deliver a stable user experience the customer by having a logical single tenant architecture: (c) ServiceNow/CDI's application development which has a paramount focus on quality, security, and the user experience is closely connected to the operations of delivering the applications in a reliable and secure cloud environment; (d) CDI invest in a comprehensive compliance strategy that allows its customers to attain their own compliance the applications laws by obtaining attestations and certifications and running its subscription service from paired data centers situated close to where its customers are located; and (e) CDI's homogeneous environment where all applications are on a single platform offers CDI a competitive advantage in being able to concentrate its efforts to make the customer's user experience the best possible.

The Data Security Guide describes the measures CDI takes to protect Customer Data when it resides in the CDI cloud. 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 and conditions of the Agreement. Capitalized terms that are not otherwise defined herein shall have the meaning given to them is the Agreement.

1. SECURITY PROGRAM

While providing the Subscription Service, CDI shall maintain a written information security program of policies, procedures, and controls ("**Security Program**") governing the processing, storage, transmission and security of Customer Data. The Security Program includes industry standard practices designed to protect Customer Data from unauthorized access, acquisition, use, disclosure, or destruction. CDI may periodically review and update the Security Program to address new and evolving security technologies, changes to industry standard practices, and changing security threats, provided that any such update does not materially reduce the commitments, protections or overall level of service provided to the Customer as described herein.

2. CERTIFICATIONS AND ATTESTATIONS

2.1. Certifications and Attestations. CDI shall establish and maintain sufficient controls to meet the objectives stated in ISO 27001 and SSAE 16 / 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, CDI shall perform an assessment against such Standards ("**Assessment**"). Upon Customer's written request, which shall be no more than once per year, CDI shall provide a summary of the Assessment(s) to Customer. Assessments shall be Confidential Information of CDI.

2.2. Safe Harbor. ServiceNow/CDI shall maintain self-certified compliance under the U.S-EU and U.US-Swiss Safe Harbor Frameworks developed by the U.S. Department of Commerce regarding the collection, use and retention of Personal Data (defined in Section 6 below) from European Union member countries and Switzerland.

3. PHYSICAL, TECHNICAL AND ADMINISTRATIVE SECURITY MEASURES

The Security Program shall include the following physical, technical and administrative measures designed to protect Customer Data from unauthorized access, acquisiton, use, disclosure, or destructions:

3.1. Physical Sercurity Measures

(a) 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 (for example, 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

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

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

3.2 Technical Security Measures

(a) Access Administation. Access to the Subscription Service by CDI employees and contrators is protected by authentication and Authorization mechanisms. User authentication is required to gain access to production and sub-productiong systems. Access privileges are based on job requirements and are revoked upon termination of employment or consulting relation. Production infrastructrue includes appropriate user account and password controls (for example, the required use of virtual private network connections, complex passwords with expiration dates, and a two-factored authenticated connection) and is accessible for administration.

(b) Logging and Monitoring. The production infrastructure log activies are centrally collected and are scured in an effort to prevent tampering and are monitored for anomailes by a trained sercurity team.

(c) Firewall System. An industry-standard firewall is installed and managed to protect CDI systms by residing on the network to inspect all ingress connections routed to the CDI environment.

(d) Vulnerability Management. CDI 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, CDI will obtain the patch from the applicable vendor and apply it within an appropriate timeframe in accordance with CDI's then current vulnerability management and sercurity patch management standard operating procedure and only after such patch is tested and determined to be safe for installation in all production systems

(e) Antivirus. CDI updates anti- virus, anti-malware, and anti-spyware sftware on regular intervals and centrally logs events for effectiveness of such software.

(f) Change Control. CDI ensures that changes to platform, applications and production infrastructure are evaluated to minimize risk and are impletmented following ServiceNow/CDI's standard operation procedure.

3.3 Administrative Sercurity Measures

(a) Data Center Inspections. CDI performs routine reviews at each data center to ensure the it contines to maintain the sercurity controls necessary to comply with the Sercurity Program.

(b) Personnel Sercurity. CDI performs background and drug screening on all employees and all contractors who have access to Customer Data in accordance with CDI's then current applicable standard operating procedure and subject tp applicable law.

(c) Sercurity Awareness and Training. CDI maintains security awareness program that includes approriate training of CDI personnel on the Sercurity Program. Training is conducted at time of hire and periodically throughout employment at CDI.

(d) Vendor Risk Management. CDI 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.

4. DATA PROTECTION AND SERVICE CONTINUITY

4.1. Data Centers; Data Backup. ServieNow shall host Customer's instances in primary and secondary SSAE 16 Type ll or ISO 27001 certified (or equivalent) data centers in the grographic regions specified on the Order Form for the Subscription Term. Each data center includes full redundancy (N+1) and fault tolerrant infrastructure for electrical, cooling and network systems. The deployed servers are enterprise scale servers are replicated in near real time to a mirrored data center in a different grographic region. Each customer instance is supported by a network configuration with multiple connections to the Internet. CDI backs up all Customer Data in accordance with CDI's standard operation procedure.

4.2. Personnal. 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 CDI telephone support representative, geographically located to ensure business continuity for support operations.

5. INCIDENT MANAGEMENT AND BREACH NOTIFICATION

5.1. Incident Monitoring and Management. CDI shall monitor, analyze and respond to security incidents in a timely manner in accordance with CDI's standard operating procedure. Depending on the nature of the incident, CDI sercurity group will escalate and engage response teams necessary to address an incident.

5.2. Breach Notification. Unless notification is delayed by the actions or demands of a law enforcement agency, CDI shall report to Customer the unauthorized by CDI that a Breach occureed. The initial report shall be made to Customer security contact(s) designated in CDI's customer support portal. CDI shall take reasonable measures to promptly mitigate the cause of the Breach and shall take reasonable corrective measures to prevent future Breaches. As information is collected or otherwise becomes available to CDI and unless prohibited by law, CDI shall provide information regarding the nature and consequences of the Breaches that are reasonably requested to allow Customer to notify affected individuals, government agencies and/or credit bureaus. Customer is soley responsible for determining whether to notify impacted Data Subjects (defined in 6.1 below) and for providing such notice, and for determining if regulatory bodies or enforcement commissions applicable to Customer or Customer Data need to be notified of a Breach.

5.3. Customer Cooperation. Customer agrees to cooperate with CDI in maintaining accurate contact information in the customer support portal and by providing any information that is reasonably requested to resolve any sercurity incident, identify its root cause(s) and prevent a recurrence.

6. DATA PROCESSING GUDELINES; COMPLIANCE WITH LAWS

6.1. Customer as Data Controller. Customer acknowledges that in relation to Personal Data supplied and/or processed under the Agreement it acts as Controller and it warrants that it will duly observe all of its obligations under all applicable laws and reguations of the European Union, the European Economic Area and their members states regarding the processing of Personal Data (collectively referred to as "Data Protection Laws") including, without limitation, obtaining and maintaining all necessary notifications and obtaining and maintaining all necessary Data Subject Consents. Customer shall (i) have sole responsibility for the accuracy, quality, integrity, legality and reliability of Personal Data and of the means by which is acquired Personal Data, (ii) ensure that data processing instructions given to CDI comply with application Data Protection Laws, and (iii) comply with all applicable Data Protection Laws in collection, compiling, storing, accessing and using Personal Data in connection with the Subscription Service. For the purposes of the Data Sercrity Guide, "Personal Data", "Controller", "Data Subject" , and "Data Subject Constent" shall have the meaning given to these terms in Driective 95/46EC. For clarity, "process" or "processing" means any operation or set of operations performed upon Customer Data.

6.2. CDI as Data Processor. CDI shall process or otherwise use Personal Data (including possible onward transfers) on behalf of Customer solely for the purpose of providing the services described in the Agreement and only in accordance with Customer's lawful instructions (limited to those instructions which CDI can reasonably carry out in the provision of the Subscription Service), the terms of the Agreement, and this Data Sercurity Guide. CDI shall ensure that those employees to whom it grants access to such Personal Data are directed to keep such Personal Data confindential and are informed of any additional data protection obligations applicable to such Personal Data. CDI shall, to the extent legally permitted, promptly notify Customer with respect to any request or communication CDI receives from any regulatory authority in relation to any data processing activies CDI conducts on behalf of Customer. In addiition, CDI will cooperate and assist Customers, at Customer's cost, in relation to any such request and to any reponse to any such communication. CDI will pass on to the Customer any request of a Data Subject to access, delete, correct, or block Personal Data processed under the Agreement. If CDI is compelled by law to disclose Customer's information as part of a civil proceeding to which Customer is a party, and Customer is not contesting

the disclosure, Customer will reimburse CDI for its reasonable cost of compiling and providing secure access to that information.

6.3. Subcontractors. CDI may engage subcontractors for processing Customer Data under the Agreement, provided CDI shall ensure compliance by such subcontractor(s) with the requirements of this Section 6 by enterinng into written agreements with such subcontractors which provide that the subcontractor will aply the Safe Harbor principles to the processing of Personal Data. CDI's use of any subcontractor will not relieve, waive, or diminish any obligation CDI has under the Agreement or this Data Security Guide.

7. PENETRATION TESTS

7.1. By a Third Party. CDI contracts with thrid party vendors to perform an annual penetration test on the CDI platform to identify risks and remediation that help increase security.

7.2. By Customer. No more than once per calendr year Customer may request to perform, at its own expense, an application penetration test of its instances of the Subcription Service. Customer shall notify CDI in advance of any test by submitting a request using CDI's online support portal and completing a penetration testing agreement. CDI and Customer must agrees upon a mutually accpetable time for the test; and Customer shall not perfom a penetration test without CDI's express written authorization. The test must be reasonable duration, and must not interfere with CDI's day-to-day operations. Promptly upom compltion of the penetration test, Customer shall provide CDI with the test results including any detected vulnerability. Upon such notice, CDI shall, consistent with industry standard practices, use all commercially reasonable efforts to promptly make any necessary changes t improve the security of the Subscription Serives. Customer shall treat test results as Confidential Information of CDI.

8. SHARING THE SECURITY RESPONSIBILITY

8.1. Product Capabilites. The Subscription Service has the capabilities to: (i) authenticate users before access; (ii) encrypt passwords; (iii) allow users to managed passwords; and (iv) prevent access by users with an inactive account. Customer manages each user's access to and use of the Subcription Serivce by assigning to each user a credential and user type that controls the level of access the the Subscription Service.

8.2. Customer Responsibilites. CDI provides the cloud environment that ermits Customer to use and process Customer Data in the Subscription Service. The architecture in the Subscription Service includes, without limitation, column level encryption functionality and the access control list engine. Customer shall be responsible or using column level encryption functionality and access control list engine for protecting all Customer Data containing sensitive data, including without limitation, credit card number, social security numbers, financial and health information, and sensitiive personal data. Customer is solely responsible for the results of its decision not the encrypt such sensitive data. CDI protects all Customer Data in the CDI cloud infrastructure equally in accordance with this Data Sercurity Guide, regardless of the classification of the type of Customer Data. Customer shall be responsible for protecting the confidentiality of each user's login and password and shall manage each user's access to the Subscription Serivce.

8.3. Customer Cooperation. Customer shall promptly apply any application upgrade that CDI determines in necessary to maintain the security, performance or availability of the Subscription Service.

8.4. Limitation. Notwithstanding anything, the contrary in the Agreement or this Data Security Guide, CDI's obligations extend only to those systems, networks, network devices, facilities and components over which CDI exercises control. The Data Security Guide does not apply to: (i) information shared with CDI that is not data stored in its systems using the Subscription Service; (ii) data in Customer's virtual private network (VPN) or a third party network; or (iii) any data processed by Customer or its users in violation of the Agreement or the Data Security Guide.