LIGHTSTEP SECURITY ADDENDUM

This Lightstep Security Addendum ("**Lightstep Security Addendum**") modifies the terms and conditions of the Agreement solely for use of the Lightstep Service during the Subscription Term. In the event of any inconsistency or conflict between this Lightstep Security Addendum and the Agreement or the Order Form, the terms and conditions of this Lightstep Security Addendum shall control with respect to the Lightstep Service. Unless otherwise specified below, all capitalized terms defined herein shall have the same meaning as set forth in the Agreement. This Lightstep Security Addendum only applies to the Lightstep Service and does not apply to other ServiceNow offerings specified on the Order Form (if any).

1. SECURITY PROGRAM

ServiceNow, will maintain a written information security program of policies, procedures and controls aligned to ISO27000 Series, or substantially equivalent standard, governing the processing, storage, transmission, and security of Customer Data in the Lightstep Service (the "**Security Program**"). A Chief Information Security Officer will be designated as responsible for coordinating, managing, and monitoring the information security function, policies, and procedures. Sufficient controls to meet certification and attestation for the objectives stated in SOC 2 Type 2 (or equivalent standards) shall be maintained for the Security Program.

2. PHYSICAL, TECHNICAL, AND ORGANIZATIONAL SECURITY MEASURES

2.1 PHYSICAL SECURITY MEASURES. The Lightstep Service data center facilities include (1) either a SOC 1 attestations or ISO 27001 certificate; (2) physical access restrictions and monitoring that include a combination of any of the following: multi-zone security, man-traps, appropriate perimeter deterrents (e.g. fencing, berms, guarded gates), on-site guards, biometric controls, CCTV, and secure cages; and (3) fire detection and fire suppression systems both localized and throughout the data center floor.

2.2 TECHNICAL SECURITY MEASURES. Infrastructure access includes appropriate user account and authentication controls. The production infrastructure log activities are secured in a manner designed to prevent tampering and are monitored for anomalies by a trained security team. An industry-standard firewall is installed and managed to protect systems by residing on the network to inspect ingress connections routed to the Lightstep Service. Industry standard encryption to encrypt Customer Data in transit over public networks will be used.

2.3 ORGANIZATIONAL SECURITY MEASURES; SERVICE CONTINUITY. Background screening will be performed on all ServiceNow employees and contractors who have access to Customer Data in accordance with operating procedures and applicable law. Security and privacy awareness training will be performed for ServiceNow employees and contractors who have access to Customer Data. Access privileges are based on job requirements. Access to systems and data are limited to personnel required to undertake their duties and are revoked upon termination of employment or consulting relationships. Data backups are performed in accordance with ServiceNow's standard operating procedures.

3. MONITORING AND INCIDENT MANAGEMENT

3.1 MONITORING AND INCIDENT MANAGEMENT. Infrastructure activity on the Lightstep Service will be (i) monitored and analyzed for security incidents, and (ii) responded to in a timely manner in accordance with ServiceNow's then-current standard operating procedure. Response teams will be engaged as may be necessary to address a security incident. ServiceNow shall not be required to inform Customer of additional security measures adopted to mitigate the cause of a security incident.

3.2 COOKIES. The Lightstep Service uses cookies to provide necessary functionality.

4. PENETRATION TESTS.

Third-party vendors are contracted to perform a penetration test on the Lightstep Service annually to identify vulnerabilities and remediation options. Executive reports from the penetration testing will be available to Customer upon written request.

5. SHARING THE SECURITY RESPONSIBILITY

5.1 SERVICE CAPABILITIES. The Lightstep Service includes a variety of security settings that allow Customers to configure security for their own use. The Lightstep Service allows, among other things, Customer to: (a) authenticate users before accessing the Lightstep Service; and (b) encrypt passwords. Customer manages each user's access to and use of the Lightstep Service by assigning to each user a credential and user role that controls the level of access to the Lightstep Service. Customer is responsible for protecting the confidentiality of each user's login and password and managing each user's access to the Lightstep Service. To the extent ServiceNow makes available to Customer documented best practices for securing Customer's use of the Lightstep Service, Customer shall be responsible for implementing such best practices for securing its use of the Lightstep Service.

5.2 LIMITATIONS. Notwithstanding anything to the contrary in this Lightstep Security Addendum or other parts of the Agreement, ServiceNow's obligations herein are only applicable to the Lightstep Service. This Lightstep Security Addendum does not apply to: (a) information shared with ServiceNow that is not Customer Data; (b) data in Customer's VPN or a third-party network; and (c) any data processed by Customer or its users in violation of the Agreement or this Lightstep Security Addendum.

6. OTHER TERMS

Except as provided in this Lightstep Security Addendum, any terms in the Agreement providing a commitment to maintain certifications such as NIST, ISO, SOC, SSAE standards, to provide encryption functionalities or to provide Customer or third party audit rights shall not apply to the Lightstep Service.