Messaging Service Security Overview

1. This Messaging Service Security Overview (referred to herein as "***Security Overview***") forms a part of the Messaging Service Ordering Agreement.

2. **Purpose.** The purpose of this Security Overview is to describe the security program for the Messaging Service. This Security Overview describes the minimum security standards that the Messaging Service maintains to protect Customer Data (as defined in the Agreement) from unauthorized use, access, disclosure, theft, or manipulation. In addition to this Security Overview, Twilio's API security documentation is available at https://www.twilio.com/docs/api/security. This Security Overview may be updated from time to time; provided, however, any update will not materially reduce the overall protections set forth in this Security Overview. Any capitalized term not defined in this Security Overview will have the meaning given in the Agreement or the Messaging Service Privacy Exhibit.

3. **Services Covered.** This Security Overview describes the architecture, administrative, technical and physical controls as well as third party security audit certifications that are applicable to the Messaging Service. Beta Offerings and any services provided by telecommunication providers involved in routing and connecting Customer communications are not covered by this Security Overview.

4. **Security Organization & Program.** The Messaging Service will maintain a risk-based assessment security program. The framework for the security program includes administrative, technical, and physical safeguards reasonably designed to protect the confidentiality, integrity, and availability of Customer Data. The security program is intended to be appropriate to the nature of Messaging Service, size and the complexity of the Messaging Service' business operations. The security framework for the Messaging Service is based on the ISO 27001 Information Security Management System and includes programs covering: Policies and Procedures, Asset Management, Access Management, Cryptography, Physical Security, Operations Security, Communications Security, Business Continuity Security, People Security, Product Security, Cloud and Network Infrastructure Security, Security Compliance, Third-Party Security, Vulnerability Management, as well as Security Monitoring and Incident Response. ServiceNow shall require that information security policies and standards are (1) reviewed and approved by Twilio management at least annually, (2) are made available to all Twilio employees for their reference, and (3) include appropriate ramifications for non-compliance.

5. **Confidentiality.** ServiceNow shall require that all Twilio employees and contract personnel are bound by Twilio's internal policies regarding maintaining confidentiality of Customer Data and contractually commit to these obligations.

6. People Security.

6.1. Employee Background Checks. ServiceNow shall require that Twilio carries out background checks on individuals joining Twilio in accordance with applicable local Law.

6.2. Employee Training. ServiceNow shall require that, at least once a year, all Twilio employees must complete the Twilio security and privacy training which covers Twilio's security policies, security best practices, and privacy principles. Employees on a leave of absence may have additional time to complete this annual training.

7. Third Party Vendor Management.

7.1. Vendor Assessment. Customer agrees that Twilio may use third party vendors to provide the Messaging Service. ServiceNow shall require that Twilio carry out a security risk-based assessment of prospective vendors before working with those vendors to validate that prospective vendors meet Twilio's security requirements. ServiceNow shall require Twilio to periodically reviews each vendor in light of Twilio's security and business continuity standards, including the type of access and classification of data being accessed (if any), controls necessary to protect data, and legal/regulatory requirements. For the avoidance of doubt, telecommunication providers are not considered subcontractors under this Agreement.

7.2 Vendor Agreements. ServiceNow shall require Twilio to enter into written agreements with all of its Vendors which include confidentiality, privacy and security obligations that provide an appropriate level of protection for the personal data contained within the Customer Data that these Vendors may process.

8. Security Certificates.

8.1. Twilio Certificates.

Twilio has obtained the following security-related certifications for the Messaging Service:

● **ISO/IEC 27001:2013 certification**. ISO 27001 is an information security standard originally published in 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). In September 2013, ISO 27001:2013 was published, and it supersedes the original 2005 standard. ISO 27001 is a globally recognized, standards-based approach to security that outlines requirements for an organization's information security management system (ISMS).

● **System and Organization Control ("SOC") 2 - Type II**. Twilio maintains SOC 2 - Type II certification for the Messaging Service described as two factor authentication service or otherwise named Authy.. SOC 2 audits for the Messaging Service are conducted once a year by an independent third-party auditor. The SOC 2 audits validate Twilio's physical and environmental safeguards for production data centers, backup and recovery procedures, software development processes, and logical security controls.

● **Payment Card Industry Data Security Standard ("PCI DSS")**. PCI DSS is a proprietary information security standard administered by the PCI Security Standards Council. PCI DSS applies to all entities that store, process or transmit cardholder data and/or sensitive authentication data including merchants, processors, acquirers, issuers, and service providers. The PCI DSS is mandated by the card brands and administered by the Payment Card Industry Security Standards Council. For more information, or to request the PCI DSS Attestation of Compliance and Responsibility Summary, see https://www.pcisecuritystandards.org/pci_security.

8.2. AWS Certifications. In addition, the Messaging Service use and leverage AWS data centers. Twilio uses and leverages AWS data centers, with a reputation of being highly scalable, secure, and reliable. Information about AWS audit certifications are available at AWS Security website https://aws.amazon.com/security and AWS Compliance website https://aws.amazon.com/compliance.

9. Architecture and Data Segregation.

Twilio Services. The cloud communication platform for the Messaging Service is hosted by Amazon Web Services ("***AWS***"). The current location of the AWS data center infrastructure used in providing Messaging Service is located in the United States. Further information about security provided by AWS is available from the AWS security webpage available at https://aws.amazon.com/security. In addition, the overview of AWS's security process is available at https://aws.amazon.com/whitepapers/overview-of-security-processes. Twilio's production environment within AWS, where Customer Data and customer-facing applications sit, is a logically isolated Virtual Private Cloud (VPC).

For Messaging Service, all network access between production hosts is restricted, using firewalls to allow only authorized services to interact in the production network. Firewalls are in use to manage network segregation between different security zones in the production and corporate environments. Firewall rules are reviewed quarterly. Twilio separates Customer Data using logical identifiers tagging all communications data with the associated Customer ID to clearly identify ownership. Twilio's APIs are designed and built to designed and built to identify and allow access only to and from these tags and enforce access controls to ensure the confidentiality and integrity requirements for each Customer are appropriately addressed. These controls are in place so one customer's communications cannot be accessed by another customer.

10. **Physical Security.** AWS data centers that host Messaging Service are strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff. These facilities are designed to withstand adverse weather and other reasonably predictable natural conditions. Each data center has redundant electrical power systems that are available twenty-

four (24) hours a day, seven (7) days a week. Uninterruptible power supplies and on-site generators are available to provide back-up power in the event of an electrical failure. More details about the physical security of AWS data centers used by Twilio for the Messaging Service, are available at https://aws.amazon.com/whitepapers/overview-of-security-processes. In addition, Twilio headquarters and office spaces have a physical security program that manages visitors, building entrances, CCTVs (closed circuit television), and overall office security. All employees, contractors and visitors are required to wear identification badges.

11. **Security by Design.** The Twilio Security Development Lifecycle (TSDL) standard defines the process by which Twilio creates secure products and the activities that the product teams must perform at different stages of development (requirements, design, implementation, and deployment). Twilio security engineers perform numerous security activities for the Services including:

- internal security reviews before products are launched;
- at least annual penetration tests performed by independent third-party contractors on all generally available products of both the network and application layer; and
- at least annually conduct threat models for the Twilio Services including documenting any detection of attacks.

12. **Access Controls.**

12.1. Provisioning Access. To minimize the risk of data exposure, ServiceNow shall require Twilio to follow the principles of least privilege through a team-based-access-control model when provisioning system access. Twilio personnel are authorized to access Customer Data based on their job function, role and responsibilities, and such access requires approval of the employee's manager. Access rights to production environments are reviewed at least quarterly. An employee's access to Customer Data is removed within 24 hours upon termination of their employment. In order to access the production environment, an authorized user must have a unique username and password, multi-factor authentication and be connected to Twilio's Virtual Private Network (VPN). Before an engineer is granted access to the production environment, access must be approved by management and the engineer is required to complete internal trainings for such access including trainings on the relevant team's systems. Twilio logs high risk actions and changes in the production environment. Twilio leverages automation to identify any deviation from internal technical standards that could indicate anomalous/unauthorized activity to raise an alert within minutes of a configuration change.

12.2. Password Controls. Twilio's current policy for employee password management follows the NIST 800-63B guidance. For the SendGrid Services, password requirements include a 10 character minimum, with at least three of the following characteristics: upper case letter, lower case letter, number, special character. When a Customer logs into its Twilio account, Twilio hashes the credentials of the user before it is stored. A customer may also require its users to add another layer of security to their account by using two-factor authentication (2FA).

13. **Change Management.** ServiceNow shall require Twilio to implement a formal change management process to manage changes to software, applications and system software that will be deployed within the production environment. Change requests are documented using a formal, auditable, system of record. Prior to a high-risk change being made, an assessment is carried out to consider the impact and risk of a requested change, evidence acknowledging applicable testing for the change, approval of deployment into production by appropriate approvers(s) and roll back procedures. A change is reviewed and tested before being deployed to production.

14. **Encryption in Transit.** For the Twilio Services, Twilio's cloud platform supports TLS 1.2 to encrypt network traffic transmitted between a Customer application and Twilio's cloud infrastructure. For the SendGrid Services, Twilio utilizes opportunistic TLS to transmit Customer's emails. This means that if Customer opts to use TLS, such email is encrypted end-to-end on the wire provided that the recipient's email service provider supports TLS.

15. **Vulnerability Management.** ServiceNow shall require Twilio to maintain controls and policies to mitigate the risk from security vulnerabilities in a measurable time frame that balances risk and the business/operational requirements. Twilio uses a third-party tool to conduct vulnerability scans at least monthly to assess vulnerabilities in Twilio's cloud infrastructure and corporate systems. Critical software patches are evaluated, tested and applied proactively. For the Messaging Service, operating system patches are applied through the regeneration of a base virtual-machine image and deployed to all nodes in the Twilio cluster over a predefined schedule. For patches Twilio has reasonably

determined are high-risk to its environment, ServiceNow shall require Twilio to deploy directly to existing nodes through internally developed orchestration tools within 30 days of a patch being made available.

16. **Penetration Testing.** ServiceNow shall require Twilio to perform penetration tests and engages independent third-party entities to conduct application-level penetration tests. Results of penetration tests are prioritized, triaged and remediated promptly by Twilio's security team.

17. **Security Incident Management.** ServiceNow shall require Twilio to maintain security incident management policies and procedures in accordance with NIST SP 800-61. Twilio Security Incident Response Team (T-SIRT), assesses the threat of all relevant vulnerabilities or security incidents and establishes remediation and mitigation actions for all events. ServiceNow shall require Twilio to retain security logs for 180 days. Access to these security logs is limited to T-SIRT. Twilio utilizes AWS platforms and third-party tools to detect, mitigate, and to help prevent Distributed Denial of Service attacks (DDoS) attacks.

18. **Resilience and Service Continuity.** Twilio infrastructure for the Messaging Service uses a variety of tools and mechanism to achieve high availability and resiliency. For the Messaging Service, Twilio's infrastructure spans multiple fault-independent AWS availability zones in geographic regions physically separated from one another. For the Messaging Service, there are manual or automatic capabilities to re-route and regenerate hosts within Twilio's infrastructure. Twilio's infrastructure is able to detect and route around issues experienced by hosts or even whole data centers in real time and employ orchestration tooling that has the ability to regenerate hosts, building them from the latest backup. Twilio leverages specialized tools that monitor server performance, data, and traffic load capacity within each availability zone and colocation data centers. If suboptimal server performance or overloaded capacity is detected on a server within an availability zone or colocation data center, then these specialized tools will increase the capacity or shift traffic to relieve any suboptimal server performance or capacity overload. Twilio will also be notified immediately and have the ability to take prompt action to correct the cause(s) behind these issues if the specialized tools are unable to do so.

19. **Backups and Recovery.** ServiceNow shall require Twilio to perform regular backups of Twilio account information, call records, call recordings and other critical data using Amazon cloud storage. Backup data are retained redundantly across availability zones and are encrypted in transit and at rest using 256-bit Advanced Encryption Standard (AES-256) server-side encryption. All cryptographic keys shall be stored in a cryptographic purpose appliance with a minimum of FIPS 140-2 level 3 compliant hardware security module "HSM". Access to the HSM shall be dual control with logging and monitoring in place to protect the confidentiality and integrity of the cryptographic keys. ServiceNow shall require Twilio to implement a high availability architecture for storing cryptographic keys for availability.

20. **Configuration Management**. ServiceNow shall require Twilio to: (a) implement and maintain standard hardened configurations for all system components within the Service; and (b) use industry standard hardening guides, such as guides from the Center for Internet Security, when developing standard hardening configurations.

21. **Software and Asset Inventory**. ServiceNow shall require Twilio to maintain an inventory of all software components (including, but not limited to, open source software) used in the Service, and inventory all media and equipment where Customer Data is stored.

22. **Workstation Security**. ServiceNow shall require that Twilio: (a) implement and maintain security mechanisms on personnel workstations, including firewalls, anti-virus, and full disk encryption; and (b) restrict personnel from disabling security mechanisms. Customer Data is not permitted to be stored on workstations or any portable storage device without ServiceNow's explicit permission.

23. Upon request by Customer, ServiceNow will provide executive summaries of an applicable penetration test.