Print this page

Customer and Partner Agreements

Privacy

Mobile Application Terms

Supplier Agreements

Intellectual Property

Resources for Law Enforcement

Civil Requests

Code of Conduct & Ethics Hotline

Digital Promotions General Rules

Customer Research and User Experience

Legal Notices for Twilio's Web Site

Italy ALIAS Database Code of Conduct

Security Overview

Last Updated: July 14, 2022

This Twilio Security Overview ("***Security Overview***") is incorporated into and made a part of the agreement between Twilio and Customer covering Customer's use of the Services (as defined below) ("***Agreement***").

1. Definitions

"***Segment Services***" means any services or application programming interfaces branded as "Segment" or "Twilio Segment".

"***SendGrid Services***" means any services or application programming interfaces branded as "SendGrid" or "Twilio SendGrid".

"***Services***" means, for the purposes of this Security Overview, collectively, the Twilio Services (as defined below), SendGrid Services, and Segment Services.

"***Twilio Services***" means any services or application programming interfaces branded as "Twilio". For the avoidance of doubt, this Security Overview does not apply to any mobile identification and authentication services branded as "Twilio" ("***Identity Verification Services***"). The security overview for the Identity Verification Services is available at https://www.twilio.com/legal/service-country-specific-terms/identity-verification/security-overview.

2. Purpose. This Security Overview describes Twilio's security program, security certifications, and technical and organizational security controls to protect (a) Customer Data from unauthorized use, access, disclosure, or theft and (b) the Services. As security threats change, Twilio continues to update its security program and strategy to help protect Customer Data and the Services. As such, Twilio reserves the right to update this Security Overview from time to time; provided, however, any update will not materially reduce the overall protections set forth in this Security Overview. The then-current terms of this Security Overview are available at https://www.twilio.com/legal/security-overview. This Security Overview does not apply to any (a) Services that are identified as alpha, beta, not generally available, limited release, developer preview, or any similar Services offered by Twilio or (b) communications services provided by telecommunications providers.

3. Security Organization and Program. Twilio maintains a risk-based assessment security program. The framework for Twilio's security program includes administrative, organizational, technical, and physical safeguards reasonably designed to protect the Services and confidentiality, integrity, and availability of Customer Data. Twilio's security program is intended to be appropriate to the nature of the Services and the size and complexity of Twilio's business operations. Twilio has separate and dedicated Information Security teams that manage Twilio's security program. There is a team that facilitates and supports independent audits and assessments performed by third parties. Twilio's security framework 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 Disaster Recovery Security, People Security, Product Security, Cloud and Network Infrastructure Security, Security Compliance, Third-Party Security, Vulnerability Management, and Security Monitoring and Incident Response. Security is managed at the highest levels of the company, with Twilio's Chief Information Security Officer (CISO) meeting with executive management regularly to discuss issues and coordinate company-wide security initiatives. Information security policies and standards are reviewed and approved by management at least annually and are made available to all Twilio employees for their reference.

4. Confidentiality. Twilio has controls in place to maintain the confidentiality of Customer Data in accordance with the Agreement. All Twilio employees and contract personnel are bound by Twilio's internal policies regarding maintaining the confidentiality of Customer Data and are contractually obligated to comply with these obligations.

5. People Security

5.1 Employee Background Checks. Twilio performs background checks on all new employees at the time of hire in accordance with applicable local laws. Twilio currently verifies a new employee's education and previous employment and performs reference checks. Where permitted by applicable law, Twilio may also conduct criminal, credit, immigration, and security checks depending on the nature and scope of a new employee's role.

5.2 Employee Training. At least once (1) per year, Twilio employees must complete a 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. Twilio’s dedicated security team also performs phishing awareness campaigns and communicates emerging threats to employees. Twilio has also established an anonymous hotline for employees to report any unethical behavior where anonymous reporting is legally permitted.

6. Third Party Vendor Management

6.1 Vendor Assessment. Twilio may use third party vendors to provide the Services. Twilio carries out a security risk-based assessment of prospective vendors before working with them to validate they meet Twilio’s security requirements. Twilio 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 or regulatory requirements. Twilio ensures that Customer Data is returned and/or deleted at the end of a vendor relationship. For the avoidance of doubt, telecommunication providers are not considered subcontractors or third-party vendors of Twilio.

6.2 Vendor Agreements. Twilio enters into written agreements with all of its vendors which include confidentiality, privacy, and security obligations that provide an appropriate level of protection for Customer Data that these vendors may process.

7. Security Certifications and Attestations. Twilio holds the following security-related certifications and attestations:

Certification or Attestation:	Covered Services:
ISO/IEC 27001	Twilio Services Segment Services
ISO/IEC 27017 & 27018	Twilio Services Segment Services
SOC 2 Type 2 (Trust Service Principles: Security & Availability)	The following Twilio Services: Programmable Voice, Programmable Messaging, Programmable Video, Twilio Flex, Lookup, Verify, Studio, Conversations, and Authy SendGrid Services Segment Services
PCI DSS Level 1	The following Twilio Services: Programmable Voice

PCI DSS Level 4	SendGrid Services

8. Hosting Architecture and Data Segregation

8.1 Amazon Web Services and Google Cloud Platform.The Twilio Services and Segment Services are hosted on Amazon Web Services ("***AWS***") in the United States of America and protected by the security and environmental controls of Amazon. The production environment within AWS where the Twilio Services and Segment Services and Customer Data are hosted are logically isolated in a Virtual Private Cloud (VPC). Customer Data stored within AWS is encrypted at all times. AWS does not have access to unencrypted Customer Data. More information about AWS security is available at https://aws.amazon.com/security/ and https://aws.amazon.com/compliance/shared-responsibility-model/ . For AWS SOC Reports, please see https://aws.amazon.com/compliance/soc-faqs/ . The Segment Services are also hosted on Google Cloud Platform ("***GCP***") in the United States of America. The production environment within GCP where the Segment Services and Customer Data are hosted are logically isolated in a Virtual Private Cloud (VPC). Customer Data stored within GCP is encrypted at all times. GCP does not have access to unencrypted Customer Data. More information about GCP security is available at https://cloud.google.com/architecture#security .

8.2 Zayo and Lumen. The SendGrid Services leverage colocation data centers provided by Zayo and Lumen (formerly known as Centurylink), which are located in the United by Zayo and Lumen (formerly known as CenturyLink), which are located in the United States of America. These colocation data centers do not store any Customer Data.

8.3 Services. For the Services, all network access between production hosts is restricted, using access control lists to allow only authorized services to interact in the production network. Access control lists are in use to manage network segregation between different security zones in the production and corporate environments. Access control lists are reviewed regularly. Twilio separates Customer Data using logical identifiers. Customer Data is tagged with a unique customer identifier that is assigned to segregate Customer Data ownership. The Twilio APIs are designed and built to identify and allow authorized access only to and from Customer Data identified with customer specific tags. These controls prevent other customers from having access to Customer Data.

9. Physical Security. AWS, Zayo, and Lumen data centers and GCP 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 (2FA) a minimum of two (2) 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. In addition, Twilio headquarters and office spaces have a physical security program that manages visitors, building entrances, closed circuit televisions, and overall office security. All employees, contractors, and visitors are required to wear identification badges.

10. Security by Design. Twilio follows security by design principles when it designs the Services. Twilio also applies the Twilio Secure Software Development Lifecycle (Secure SDLC) standard to perform numerous security-related activities for the Services across different phases of the product creation lifecycle from requirements gathering and product design all the way through product deployment. These activities include, but are not limited to, the performance of (a) internal security reviews before deploying new Services or code; (b) penetration tests of new Services by independent third parties; and (c) threat models for new Services to detect potential security threats and vulnerabilities.

11. Access Controls

11.1 Provisioning Access. To minimize the risk of data exposure, Twilio follows 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. Access rights to production environments that are not time-based are reviewed at least semi-annually. An employee's access to Customer Data is promptly removed upon termination of their employment. In order to access the production environment, an authorized user must have a unique username and password and multi-factor authentication enabled. Before an engineer is granted access to the production environment, access must be approved by management and the engineer is required to complete internal training for such access including training on the relevant team's complete internal training for such access including training 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.

11.2 Password Controls. Twilio's current policy for employee password management follows the NIST 800-63B guidance, and as such, our policy is to use longer passwords, with multi-factor authentication, but not require special characters or frequent changes. For SendGrid employees, password requirements include an eight (8) character minimum, with at least three (3) of the following characteristics: upper case letter, lower case letter, number, or special character. When a customer logs into its 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).

12. Change Management. Twilio has a formal change management process it follows to administer changes to the production environment for the Services, including any changes to its underlying software, applications, and systems. Each change is carefully reviewed and evaluated in a test environment before being deployed into the production environment for the Services. All changes, including the evaluation of the changes in a test environment, are documented using a formal, auditable system of record. A rigorous assessment is carried out for all high-risk changes to evaluate their impact on the overall security of the Services. Deployment approval for high-risk changes is required from the correct organizational stakeholders. Plans and procedures are also implemented in the event a deployed change needs to be rolled back to preserve the security of the Services.

event a deployed change needs to be rolled back to preserve the security of the Services.

13. Encryption. For the Twilio Services, (a) the databases that store Customer Data are encrypted using the Advanced Encryption Standard and (b) Customer Data is encrypted when in transit between Customer's software application and the Services using TLS v1.2. For the SendGrid Services, Twilio provides opportunistic TLS v1.1 or higher for emails in transit between Customer's software application and the recipient's email server. The SendGrid Services are designed to opportunistically try outbound TLS v1.1 or higher when attempting to deliver an email to a recipient. This means that if a recipient's email server accepts an inbound TLS v1.1 or higher connection, Twilio will deliver an email over a TLS encrypted connection. If a recipient's email server does not support TLS, Twilio will deliver an email over the default unencrypted connection. The SendGrid Services provide an optional feature, which Customer has to enable, that allows Customer to enforce TLS encryption. If Customer enables the enforced TLS feature, Twilio will only deliver an email to a recipient if the recipient's email server accepts an inbound TLS v1.1 or higher connection. For the Segment Services, Customer Data is encrypted at rest using the Advanced Encryption Standard.

14. Vulnerability Management. Twilio maintains controls and policies to mitigate the risk of 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 regularly to assess vulnerabilities in Twilio's cloud infrastructure and corporate systems. Critical software patches are evaluated, tested, and applied proactively. 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 high-risk patches, Twilio will deploy directly to existing nodes through internally developed orchestration tools.

15. Penetration Testing. Twilio performs penetration tests and engages independent third-party entities to conduct application-level penetration tests. Security threats and vulnerabilities that are detected are prioritized, triaged, and remediated promptly. Twilio maintains a Bug Bounty Program through Bug Crowd, which allows independent security researchers to report security threats and vulnerabilities on an ongoing basis.

16. Security Incident Management. Twilio maintains security incident management policies and procedures in accordance with NIST SP 800-61. Twilio's Security Incident Response Team (T-SIRT) assesses all relevant security threats and vulnerabilities and establishes appropriate remediation and mitigation actions. Twilio retains security logs for one hundred and eighty (180) days. Access to these security logs is limited to T-SIRT. Twilio utilizes third-party tools to detect, mitigate, and prevent Distributed Denial of Service (DDoS) attacks.

17. Discovery, Investigation, and Notification of a Security Incident. Twilio will promptly investigate a Security Incident upon discovery. To the extent permitted by applicable law, Twilio will notify Customer of a Security Incident in accordance with the Data Protection Addendum. Security Incident notifications will be provided to Customer via email to the email address designated by Customer in its account.

18. Resilience and Service Continuity

18.1 Resilience. The hosting infrastructure for the Twilio Services and Segment Services (a) spans multiple fault-independent availability zones in geographic regions physically separated from one another and (b) 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.

18.2 Service Continuity. Twilio also leverages specialized tools available within the hosting infrastructure for the Services to monitor server performance, data, and traffic load capacity within each availability zone and colocation data center. If suboptimal server performance or overloaded capacity is detected on a server within an availability zone or colocation data center, these specialized tools increase the capacity or shift traffic to relieve any suboptimal server performance or capacity overload. Twilio is also immediately notified in the event of any suboptimal server performance or overloaded capacity.

19. Customer Data Backups. Twilio performs regular backups of Customer Data, which is hosted on AWS's data center infrastructure. Customer Data that is backed up is retained redundantly across multiple availability zones and encrypted in transit and at rest using the Advanced Encryption Standard.