WHITEPAPER

Twilio cloud communications

SECURITY

twilio

From the world’s largest public companies to early-stage startups, people rely on Twilio’s cloud communications platform to exchange millions of calls and messages —every day— from web and mobile apps. These communications facilitate deliveries, power customer support, and keep mission-critical applications running nonstop. Providing reliable voice, video, and messaging is only the first step. These communications must also follow the latest security best practices and comply with strict privacy regulations and corporate policies.

The information contained in this document is intended to provide transparency on Twilio’s security stance and processes. We also cover best practices gleaned from customer implementations to help you improve and secure the applications you build with Twilio.

SECURITY ORGANIZATION & PROGRAM

While security is a high priority for all teams, a dedicated Security Team manages Twilio's security program. The Twilio security framework is based on the ISO 27001 Information Security Standard 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.

Security is represented at the highest levels of the company, with our Chief Information Security Officer meeting with executive management regularly to discuss issues and coordinate company-wide security initiatives. Information security policies and standards are approved by management and available to all Twilio employees.

PEOPLE SECURITY

The people creating Twilio products are important; we've implemented processes to ensure we're bringing in the right people and keeping them up to date on the latest security trends. Here are some of the processes we have in place:

BACKGROUND CHECKS

All candidates in the USA must pass stringent background checks by a specialized third-party before being offered a position. For domestic candidates, these checks include: SSN trace, criminal county search (7-Year address history), multi-state instant criminal, National Sex Offenders Public Registry, OFAC, professional references, and education verification. For international new hires, the background check includes (where legal): international criminal search and education verification.

INFOSEC TRAINING

All new Twilio employees attend a "Security 101" training during the onboarding process. In addition, all Twilio employees must take the Twilio Security and Privacy training once a year, which covers the Information Security Policies, security best practices, and privacy principles.

CONTINUOUS EDUCATION CAMPAIGN

The Twilio Security Team provides continuous communication on emerging threats, performs phishing awareness campaigns, and communicates with the company regularly.

ETHICS HOTLINE

Twilio implemented an anonymous[1] tip line for employees to report any unethical behavior.

[1] Twilio employees can anonymously report issues in geographies where anonymous reporting is legal

PRODUCT SECURITY

The mission of Twilio Product Security program is to enable the product teams to build solutions that are best in class when it comes to security. The following activities help us to achieve this mission:

APPLICATION SECURITY STANDARDS AND GUIDELINES

The Twilio Security Development Lifecycle (TSDL) standard defines the process by which we create secure products and the activities that the product teams must perform at different stages of development (requirements, design, implementation, and deployment).

SECURE BY DESIGN

Twilio security engineers continuously perform numerous activities to ensure that our products are secure, including:

- Internal security reviews before products are launched
- Regular penetration tests performed by third-party contractors
- Continuously running bug bounty program

- Continuously running internal and external security tests
- Regularly conducted threat models

For more information on Twilio bug bounty program, please visit: https://bugcrowd.com/twilio

BUILDING SECURITY DNA

At Twilio, we implement and conduct technology-specific software security trainings. The training material is developed in house and is highly Twilio-specific to ensure our developers get the most out of these trainings. All our developers must pass the final tests to confirm comprehension. We've also embedded security champions within our development teams to amplify the efforts of the Security Team.

CHANGE MANAGEMENT

Twilio has a formal change management process where all changes are tracked and are approved. A change is reviewed before being moved into a staging environment where it is further tested before finally being deployed to production.

ENCRYPTION IN TRANSIT

Twilio supports TLS 1.0, 1.1 and 1.2 to encrypt network traffic between the customer application and Twilio.

PENETRATION TESTING

Twilio regularly performs third-party penetration tests. Additionally, our bug bounty program encourages ongoing testing and responsible disclosure of vulnerabilities from the security community.

ACCOUNT SECURITY

Twilio secures your secrets using industry best practice methods to salt and repeatedly hash your credential before it is stored. Users can also add another layer of security to their account by using two-factor authentication (2FA) for the Twilio console.

TWILIO SECURITY DEVELOPMENT LIFECYCLE (TSDL)

Twilio's developers follow the TSDL while developing our products, ensuring products are secure by design, in development, and after they have been deployed.

CLOUD & NETWORK INFRASTRUCTURE SECURITY

The security of our infrastructure and networks is critical. Creating a safe platform for Twilio applications and customer innovation is the mission of our cloud security program.

Twilio's Cloud Security Standard (TCSS) comprises best-in-class security practices. We've open-sourced the security policy framework on which our own standard is based. All requirements in the TCSS are driven by four key principles:

ASSET MANAGEMENT AND OWNERSHIP

All cloud assets must have a defined owner, security classification, and purpose.

INFRASTRUCTURE MANAGEMENT

Direct access to infrastructure, networks, and data is minimized to the greatest extent possible. Where possible, control planes are used to manage services running in production, to reduce direct access to host infrastructure, networks, and data. Direct access to production resources is restricted to employees requiring access and requires approval, strong multifactor authentication, and access via a bastion host.

DEFENSE-IN-DEPTH

Twilio's production environment, where all customer data and customer-facing applications sit, is a logically isolated Virtual Private Cloud (VPC). Production and non-production networks are segregated. All network access between production hosts is restricted using firewalls to only allow authorized services to interact in the production network.

NETWORK MONITORING FOR TWILIO STANDARDS

Twilio logs high risk actions and changes in the production network. We leverage automation to identify any deviation from our technical standards and raise issues within minutes of the configuration change occurring.

For more information on Twilio's Cloud Security Standard, please visit: https://github.com/twilio/cloudsec

CONTINUOUS MONITORING AND VULNERABILITY MANAGEMENT

At Twilio, the security and resiliency of our products and infrastructure is a top priority. The Continuous Monitoring program builds on our "secure by design" principles. The Continuous Monitoring program develops processes and procedures for leading incidents and designing proactive and detective capabilities for the Twilio Platform. The Vulnerability Management program establishes how we identify, respond, and triage vulnerabilities against the Twilio platform. To ensure security of our platform, Twilio continues to mature the following capabilities:

CONTINUOUS MONITORING PROGRAM

Twilio approaches continuous monitoring through the development of proactive and detective capabilities. Through the ongoing awareness of vulnerabilities, incidents, and threats, Twilio is poised to respond and mitigate accordingly.

INCIDENT RESPONSE PROGRAM

Twilio maintains an incident response program in accordance to NIST SP 800-61. The program defines conditions under which security incidents are classified and triaged. Twilio Security Incident Response Team, or T-SIRT, assesses the threat of all relevant vulnerabilities or security incidents and establishes remediation and mitigation actions for all events.

SECURITY LOG RETENTION

Security logs are retained for 180 days. Access to these security logs is limited to T-SIRT

DISTRIBUTED DENIAL-OF-SERVICE (DDOS) PREVENTION

Twilio leverages industry leading platforms and T-SIRT to detect, mitigate, and prevent DDoS attacks.

PHYSICAL SECURITY

Physical security is an important part of Twilio's security strategy. We're committed to securing our facilities.

DATACENTER SECURITY

Twilio leverages AWS data centers for all production systems and customer data. AWS follows industry best practices and complies with an impressive array of standards.

For more information on AWS Data Center Physical Security, see the AWS Security Whitepaper: https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

OFFICE LOCATION SECURITY

Twilio has a security program that manages visitors, building entrances, CCTVs, and overall office security. All employees, contractors and visitors are required to wear identification badges which distinguish their respective role.

BUSINESS CONTINUITY / DISASTER RECOVERY

Twilio uses a variety of tools and mechanisms to ensure best-in-class resiliency.

RECOVERY PLANNING

Twilio maintains formal Business Continuity and Disaster Recovery plans that are regularly reviewed and updated.

GLOBAL RESILIENCY

Hosting our services on AWS gives Twilio the ability to remain resilient globally even if one location goes down. AWS spans multiple geographic regions and availability zones, which allow Twilio servers to remain resilient in the event of most failure modes, including natural disasters or system failures.

CUSTOMER DATA BACKUPS

Twilio performs regular backups of Twilio account information, call records, call recordings and other critical data using Amazon S3 cloud storage. All backups are encrypted in transit and at rest using strong encryption. Backup files are stored redundantly across multiple availability zones and are encrypted.

THIRD-PARTY SECURITY

In today's interconnected business environment, maintaining visibility into the software supply chain is of utmost importance. Twilio has implemented the following programs:

VETTING PROCESS

Third-parties used by Twilio are assessed before onboarding to validate that prospective third-parties meet Twilio's security requirements.

ONGOING MONITORING

Once a relationship has been established, Twilio periodically reviews security and business continuity concerns at existing third parties. The program takes into account the type of access and classification of data being accessed (if any), controls necessary to protect data, and legal/regulatory requirements.

OFFBOARDING

Twilio ensures that data is returned and/or deleted at the end of a vendor relationship.

SECURITY COMPLIANCE

Twilio is committed to mitigating risk and ensuring Twilio services meet regulatory and security compliance requirements:

REGULATORY ENVIRONMENT

Twilio complies with applicable legal, industry, and regulatory requirements as well as industry best practices.

TOP TIER INFRASTRUCTURE PROVIDER

Twilio's cloud communications platform is hosted at Amazon Web Services (AWS) data centers, which are highly scalable, secure, and reliable. AWS complies with leading security policies and frameworks, including SSAE 16, SOC framework, ISO 27001 and PCI DSS.

ISO 27000 SERIES

Twilio has obtained our ISO/IEC 27001:2013 certification, showing our maturity within the Information Security space. Security is a top priority for Twilio, and this achievement demonstrates our commitment to information security, data protection and continuous improvement.

EU - U.S. PRIVACY SHIELD FRAMEWORK

Twilio is self-certified under Privacy Shield as a part of our commitment to comply with EU data protection requirements when transferring personal data from the European Union to the United States.

SOC2 TYPE II

Authy (Two-Factor Authentication by Twilio) has recently completed its SOC2 Type II audit for the Trust Services Principles of Security and Availability.

SUMMARY

Twilio cloud communications platform enables businesses to deliver superior customer experiences by easily incorporating voice, video, and messaging into their customer-facing applications. Security mechanisms to protect physical, network and application components of the platform, coupled with transparency about security practices and compliance best practices, give customers the confidence they need to move communications to the cloud.

For further details and steps to secure your Twilio-powered application, check out the API docs security page. Lastly, if you have more questions, or need more detailed answers, feel free to get in touch with our Security Team via the contact form at *https://www.twilio.com/help/sales.*

API docs security details can be found here:
https://www.twilio.com/docs/api/security