Version: 1.0
Updated: 09 10 21

Twilio security

How Twilio securely delivers our trusted customer engagement platform

Contents

Overview

Twilio's trusted customer engagement platform powers over one trillion human interactions annually with flexible APIs built on a resilient infrastructure to facilitate a superior customer experience while mitigating the security risks associated with on-demand global communications at scale.

The Twilio Trust & Security team strives to maintain the confidentiality, availability, and integrity of data and services by proactively mitigating cybersecurity risks and helping customers meet regulatory demands, including data governance, privacy, and transparency.

As part of our information security management system (ISMS), Twilio services are certified under ISO/IEC 27001, a framework that provides specific requirements and practices to bring information security under management control. In addition, we have attestations to ISO/IEC 27017 and ISO/IEC 27018, internationally recognized codes of practice that provide guidance on controls to address cloud-specific information security threats and the protection of personally identifiable information (PII).

Twilio Programmable Voice, Programmable Messaging, Programmable Video, and Authy are compliant with SOC 2 Type II. Documentation of these certifications and attestations is available to contracted customers and partners on request.

To achieve this goal, we use a set of core principles to guide a strong security posture:

- **Universal participation.** We recognize that any component of the organization could be a potential avenue for compromise. Building a strong security program requires the cooperation of the entire workforce. Everyone at Twilio is responsible for the security of our platform.
- **Risk-based security.** An organization's security focus should be defined by the set of risks it faces. Maintaining focus means continually identifying and managing emerging threats and significant risks.
- **Least-privilege**. Users and systems should have the minimum level of access necessary to perform their defined functions. Unnecessary levels of access are restricted.
- **Defense-in-depth.** Overall security cannot be reliant upon a single defense mechanism. If one security control is defeated, other controls should compensate to resist the attack.
- **Secure failure.** When a system's availability, integrity, or confidentiality is compromised, the system should fail to a secure state and allow for secure recovery.
- **Effective authentication and authorization.** Establish identity for authentication and leverage role-based authorization to make informed access control decisions.
- **Audit mechanisms.** Design and implement audit mechanisms to detect unauthorized use and to support incident investigations.

This document describes the security program that protects Twilio products and the Twilio platform.

Securing our people

Our community of Twilions is the most important asset to Twilio. We make the well-being of our people a top priority by providing a safe and secure working environment. We also ask our workforce to take responsibility for learning and following good security practices.

Twilio maintains a strong security culture and ensures our people are a robust link in the security chain that protects the company, our customers, and your data. We do this by making sure all staff have the training, tools, and knowledge they need to work securely and are empowered to help others do the same.

Security is represented at the highest levels of the company. Twilio's Chief Security Officer meets regularly with executive management to discuss challenges and coordinate company-wide security initiatives. Security starts at the top and reaches every member of the workforce. Twilio employees are responsible for understanding and adhering to the guidance contained in our security policies and standards. Security policies and standards are reviewed and approved by management at least annually and are made available to the Twilio workforce for their reference.

Twilio has established an anonymous hotline for the workforce to report unethical behavior where anonymous reporting is legally permitted. Our Trust & Security team is accessible through a number of channels so that people who work for Twilio can always raise concerns or issues about any security topic, including potential security threats or incidents.

All Twilio employees and contract personnel are bound by Twilio's internal policies and standards regarding proper use and confidentiality

of customer data. The Twilio Code of Conduct explicitly addresses risks such as bribery, corruption, compliance with international trade laws, and human trafficking.

Employee background checks

A robust security posture starts with knowing your people. Twilio carries out background checks in accordance with applicable local laws. Twilio verifies a new recruit's education and previous employment, and also carries out reference checks as necessary. Depending on the role or position of a prospective employee, Twilio may also conduct criminal, credit, immigration, and security checks as allowed by local labor law or statutory regulations.

Security awareness

During onboarding, all new hires must complete Twilio's Security Awareness Training, which explains common security threats, security policies, and best practices. New hires are also required to read and agree to Twilio's Employee Handbook and complete the Twilio Code of Conduct Training, which includes information about protecting confidential information and company assets, our commitment to the privacy and integrity of customer data, and our anti-bribery and corruption policies.

The Twilio workforce is required to complete the Twilio Security Awareness Training annually and acknowledge our set of security policies and standards.

Twilio educates its workforce on protecting and securing their home networks and devices, including recommendations for Wi-Fi networks, known device attack vectors such as Bluetooth, physical security, and best practices for using software and handling data.

Some employees receive additional security training relevant to their role, such as secure development and secure design practices.

Workforce equipment

Twilio-issued laptops have disk encryption enabled to protect data at rest, and restrict mounting of external drives to prevent exfiltration of data. Twilio laptops run anti-virus and anti-malware software that uses behavior-based detection techniques to evaluate actions and potential actions for threats rather than relying on known malware byte signatures. Additionally, we deployed an insider risk monitoring solution across all Twilio-managed laptops throughout the enterprise to further reduce the risks to Twilio's sensitive information.

Passwords

Twilio's employee password policy is aligned with the NIST 800 63B guidelines. Employee passwords must be at least 16 characters in length, changed every 180 days, and cannot be the same as any of the previous 12 passwords. Accounts are locked after seven invalid login attempts. Additionally, access to most systems is centralized with the use of single sign on (SSO).

Privileged passwords are more stringent. They must be at least 20 characters in length, including at least three of the following: uppercase, lowercase, numbers, and special characters. They must be changed every 60 days and can't be the same as any of the previous 20 passwords. Multi-factor authentication (MFA) is required where possible, and accounts are locked out after three invalid login attempts.

Employee access

Twilio follows the principle of least privilege. Users and systems have the minimum level of access necessary to perform their defined function, and unnecessary levels of access are restricted. Access levels are audited quarterly, and inappropriate access is revoked. When an employee's job responsibilities change, access privileges are revoked or reassigned as needed. Upon termination, an employee's accounts are deactivated. Where technically feasible, these accounts are removed from the system. For a temporary worker or contractor, access privileges have an automatic expiration date on all accounts to guarantee that access is terminated no later than the end of the contract. Inactive user accounts are disabled after 90 days for Twilio Services.

To access production environments, Twilio engineers must complete required engineering courses and Secure Coding Training. Every engineer must have in-depth knowledge of the relevant systems and be considered a subject matter expert before being granted access to production systems.

User authentication

Only Twilio-owned devices (i.e., employee laptops) can access the production and confidential environments where Twilio confidential and customer data is stored. Employees must be connected to a trusted VPN, and for certain profiles must use multi-factor authentication to access the Twilio internal network. Wireless networks are secured using WPA2-Enterprise using RADIUS integrated with Twilio Active Directory.

Production, corporate, and other networks are physically and logically separated and assigned profiles that require appropriately restrictive levels of access. The production environment can only be accessed by authorized personnel via VPN, which requires hardware-based multi-factor authentication. Twilio production is primarily hosted on Amazon Web Services (AWS), and all access to the production environment is remote, even if a user is on the office network. Remote administration requires SSH access that is restricted in three ways: use of a bastion host, use of SSH Keys instead of passwords, and the use of Yubikey for MFA.

Web filtering

Twilio utilizes a DNS proxy filtration service that provides the first line of defense against threats on the internet. It is used to prevent access to inappropriate websites and block phishing sites wherever Twilio employees are connected to Twilio's corporate network via VPN or from within the office.

Data loss prevention

Twilio has a data loss prevention (DLP) system in place that scans for sensitive data which may potentially be exposed publicly or improperly stored and has alerting and quarantine capabilities for our primary collaboration systems.

Securing our products by design

Twilio prioritizes securing our products, services, and APIs from the start. Security is engaged at key parts of the design process to offer guidance to our engineers. The Twilio Secure Development Lifecycle

ensures products are secure by design, both in development and after they have been deployed.

Twilio Secure Development Lifecycle

The Twilio Secure Development Lifecycle defines the standards by which Twilio creates secure products and the process that product teams must perform at different stages of development (requirements, design, implementation, and deployment). Twilio security engineers support development with activities including but not limited to:

- Internal security reviews prior to product launch
- Penetration tests performed by specialized third-party firms
- Ongoing bug bounty programs
- Regular threat modeling
- Secure development training covering the OWASP Top 10
- Security Champions embedded within development teams
- Automated static and dynamic application security testing (SAST and DAST) in the CI/CD pipeline
- Automated container scanning in the CI/CD pipeline

Change management

Twilio uses a continuous software delivery model to ensure a stable production environment for our customers.

Operational change control procedures are in place for products and services within Twilio and include processes for introducing changes into the production environment. Software changes and updates follow a defined and rigorous process to ensure that changes are valuable, while minimizing risk. These change control procedures are communicated to parties who perform system maintenance and updates on Twilio assets.

In order to maintain a continuous delivery model and ensure a stable production environment, Twilio enforces a consistent change management process for software releases across the company. Twilio software must complete a series of quality-related checkpoints and pass related tests before, during, and after deployment.

Change requests are documented using a formal, auditable system of record. The change management process includes the following items:

- An assessment of impact and risk of change requested
- Evidence that applicable testing was performed successfully
- Review and approval prior to deployment into production environment
- Communication of changes to relevant people/departments
- Rollback procedures

Threat modeling

Threat models are leveraged to identify, triage, and mitigate threats against our products, services, and APIs early in the SDLC. Twilio uses a custom end-to-end threat modeling methodology that combines a traditional data-flow diagram and the STRIDE model. We prioritize protection from various attack vectors by examining services and the information they store and/or transmit. Threat modeling at Twilio is

supported by comprehensive documentation, data flow architecture, and a list of all personally identifiable information (PII) used by the application.

Product security: Champions and Partners

Security Champions bring best-in-class security to their team's products and services by ensuring new features go through security reviews. Security Champions raise the bar on security and build features that can support our customers with the highest security and data protection needs. Most product engineering teams have at least one dedicated Security Champion.

Security Partners are dedicated points of contact in the Trust & Security team who maintain knowledge and understanding of the products to assist with security reviews. Security Partners meet regularly with Security Champions, collaborating to perform threat modeling, code reviews, penetration tests and resolve security issues found through manual or automated security testing.

Bug bounty program

Twilio runs multiple public and private bug bounty programs through BugCrowd to encourage trusted security researchers from around the world to identify and report vulnerabilities for products in scope on our platform, APIs, core products, and console. We update our public bug bounty programs on a regular basis to make sure the most recent releases are being battle tested. Additionally, we review and adjust our payouts to stay competitive and have paid up to $10,000 for a single submission.

Securing data

Twilio's data governance strategy is designed to ensure data is discoverable, understandable, high-quality, usable, secure, and compliant with company policies. Our goal is to have reliable data sets to evaluate enterprise performance, make management decisions across the company, support trust and company reputation, and perform audits. Implementation of this strategy involves people, processes, and technology.

Twilio's Data Governance Program was established to ensure Twilio's information assets are formally, proactively, and effectively managed throughout the company. The program's mission is to enable Twilio employees to find, understand, trust, protect, and leverage Twilio's data assets responsibly.

Data classification

Twilio classifies data based on importance, business need, and operational risk. Classification of the different data risk profiles helps Twilio design systems that meet our business needs, reduce operational risk, and serve our customers responsibly and ethically.

Classification	Description
Secret	This is the highest level of data security classification and requires the highest level of security controls. Secret data may represent an existential threat to the company, its customers, or end users, and/or would cause exceptionally grave damage should it be compromised.
Restricted	Restricted data, if compromised, would cause severe damage to Twilio, Twilio's customers, end users, employees, former employees, customers, vendors, and/or third parties.
Confidential	Confidential data is intended for internal use only. Data that is not expressly classified as Secret, Confidential, and/or Public should be treated as Confidential data. Unauthorized disclosure, alteration, or destruction of that data could result in a moderate impact to Twilio, its customers, and/or end users.
Public	Public data is intended for external release, use by non-employees, or has been downloaded from publicly available sources free of charge. Unauthorized disclosure of Public data would result in little or no risk to Twilio, its customers, and/or end users.

Data stewardship

Twilio's data governance culture extends to all levels of the organization under a three-level pyramid model: Operational, Tactical and Strategic. At each level of the pyramid exists a relationship entity also known as a logical role.

At the Operational level, any employee who defines, produces, or consumes data is considered a Data Steward. Data Stewards have formal accountability to write data definitions or policies that follow established guidelines. Data Stewards are supported by Domain Stewards at the Tactical level.

At the Tactical Level, Domain Stewards are the logical role taking the enterprise view of data and seeking to continually improve governance. Their responsibility is to define the standards of the data in their domains, making sure the appropriate documentation is created and shared across all stakeholders. Additionally, Domain Stewards work on the classification of databases, schemas, tables, and columns according to the Twilio Data Classification Policy and identify any data structures that contain PII in accordance with the Twilio Privacy Policy.

Finally, at the Strategic level, Twilio's Data Governance Council makes the strategic decisions impacting business and technology areas of Twilio and setting the data governance strategic direction.

Credential management

Passwords and Twilio API credentials are individually salted and hashed before they are stored, using the bcrypt algorithm.

Data encryption

Twilio supports the use of TLS 1.2 to encrypt data in transit between the customer application and Twilio over public networks. Databases housing sensitive customer data are encrypted at rest.

Data segregation

Twilio has implemented logical separation between customers by tagging all communications data with the associated Customer ID to clearly identify ownership. Twilio applications are designed and built to honor these tags and enforce access controls to ensure the confidentiality requirements for each customer are met. These controls are reviewed as a part of the security assessment process to ensure one customer's communications cannot be accessed by another.

Data access

To minimize the risk of data exposure, Twilio follows the principle of least privilege through a team-based access control model when provisioning system access. Personnel access to customer data is restricted based on business need, role and appropriate approvals. Employee access to customer data is promptly removed upon termination of employment. Access rights to production environments are reviewed at least semi-annually.

Twilio employees adhere to specific data handling guidelines in conformance with the commitments in Twilio's Privacy Statement and our Binding Corporate Rules. Technical controls exist to prevent storage on removable media devices (i.e., USB flash drives, external hard drives, and any pluggable storage devices). There is a limited set of circumstances in which a Twilio employee may directly interact with customer data, including as necessary for legal holds, law enforcement requests, fraud investigations, troubleshooting or providing support.

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).

Securing our internal environment

Twilio takes a number of steps to secure our internal environment. We monitor and secure our network and infrastructure through the enforcement of security policies and controls that provide defense in depth, ensuring that a compromise in one layer is resisted by additional layers of protection.

Defense in depth

Twilio uses the defense in depth strategy to limit the "blast radius" of harm in case of an intrusion at any level. We create several layers of protection, ensuring that the failure of any single layer does not represent a loss of protection to information and assets, by securing and containing assets at the account, network, and service level to provide a protective operating environment for applications. Potentially weak services are isolated and protected to prevent their vulnerabilities from affecting other systems.

Asset management

The Twilio Enterprise Security Standard defines requirements for the protection of corporate assets and infrastructure. Assets are inventoried and documented to determine necessary security measures. Assets are reviewed regularly to make sure they continue to meet the security standards.

Infrastructure management

All Twilio-controlled enterprise networks conform to an approved security architecture. All network access for Twilio Services between production hosts is restricted, using AWS security-groups to allow only authorized services to interact in the production network. Twilio's security architecture uses technologies to segment and filter traffic between security zones. Firewalls manage network segregation between different security zones in the production and corporate environments.

Any inter-site or network connectivity is established through edge routers and security devices. All network and VPN connections terminate in edge zones. Outbound DNS requests from any zone travel through DNS resolvers and are auditable and traceable to a single device. Firewall rules allowing traffic between security zones are documented, including a business case, and are approved by the Chief Security Officer (CSO) or appointed delegate.

For our corporate systems and cloud infrastructure, Twilio assesses vulnerabilities using open source and commercial vulnerability scanning tools. We also receive alerts from third parties, including our vendors and the US CERT.

Network monitoring

Twilio network's security controls operate at the host level, and as such, we do not have a traditional DMZ. Instead, Twilio uses AWS Web Application Firewall selectively for external services with AWS Shield, while leveraging AWS Security Groups and Access Control Lists (ACLs) to manage traffic. AWS VPCs (Virtual Private Clouds) are used to manage network segregation between different security zones in the Production environment. Firewalls are used to maintain segregation of the corporate networks; rules are reviewed quarterly.

Twilio employs an intrusion detection system (IDS) to monitor access events, security-related events, and API authentication. Alerts are sent to the security staff when anomalous events are detected. Security logs are collected within a log aggregation platform. Logs are retained based on applicable regulatory requirements.

Logging and monitoring

Twilio logs high-risk actions and changes in the production network. We use automation to identify any deviation from our technical standards and raise issues within minutes of the configuration change occurring. We log users' successful and unsuccessful attempts to authenticate to the production environment.

Security logs are collected within a log aggregation platform. Logs are retained based on applicable regulatory requirements. Access to these security logs is limited to only authorized employees who need access based on their roles.

Securing our endpoints

Twilio uses an automated daily testing platform to continually monitor and secure our points of ingress and egress for edge services.
The platform sends regular reports to the appropriate teams with information necessary to respond to any incidents.

Identifying and responding to threats

Twilio maintains processes and tools to identify and respond to vulnerabilities and other threats. Twilio scans for security threats using open-source, commercial, and in-house tools.

Vulnerability detection and remediation

Twilio's Trust & Security team validates the vulnerabilities identified by these tools and processes, then rates vulnerabilities according to our risk-based vulnerability management standard. Our risk calculation is based on multiple factors including existing controls that mitigate the risk, scope, and severity of a potential exploit. Remediation actions to address vulnerabilities are applied within the timeframes assigned to risk-ratings as defined in Twilio's Vulnerability Management Standard. For critical issues, we maintain a 7-day SLA for patches, and a 14-day SLA for vulnerabilities.

Patching process
Assets are protected against known vulnerabilities by the regular application of vendor-supplied security patches and updates. Assets that rely on the use of a base image and do not support live patching are cycled or refreshed to use the latest available base image to ensure that applicable security updates are implemented on a 30-day cadence.

SOCless response automation
Security Engineering provides and supports SOCless, a Security Orchestration Automation Response (SOAR) platform as a service (PaaS). SOCless is a unique, serverless platform composed of AWS Lambda, Step Function, API Gateway, DynamoDB and other AWS infrastructure. Security Response Automation is part of the Security Department's goal of increasing the speed of event response, reducing malicious impact, and scaling with Twilio without introducing additional cost. To help other organizations defend their customers against threats at scale, and encourage the community to contribute to our efforts, we've released SOCless as an open-source project.

For more information, see Introducing Twilio's SOCless.

Identity and access management
Twilio manages user access in an auditable system throughout the entire account life cycle. Systems have at least a primary and a backup approver. For audit purposes, access requests and approvals, as well as modifications to user access, are documented and preserved for at least two years.

Identity and access management (IAM) Permissions and Security Group rules use the principle of least privilege. IAM Permissions are restricted to resources owned by the service, and limited to the specific action required. Security Group rules are restricted to individual IP addresses and services where possible. Exceptions to these requirements must have a business case and be approved by the Trust & Security team.

Security risk management

The Twilio Security Risk Management Program (RMP) is a flexible and scalable framework to assess and manage risks in the Twilio environment and provide direction and basis to refine the Twilio ISMS. As the business grows and evolves, and the competitive and regulatory environment changes, the Twilio RMP is intended to be reapplied or adapted within the organization, based on organizational context and present and future priorities.

RMP strategies evolve in accordance with business drivers for risk-based decision making and requirements for information. The risk management lifecycle defined in the Twilio RMP is adapted to manage risks in various services within Twilio and to perform functional risk assessments. Twilio top-level management is responsible for review and prioritization of exceptions, findings, and vulnerabilities.

The security risk management framework with supporting processes is used as the basis for the ongoing identification, assessment, treatment, and reporting of security risks at Twilio. Potential security risks and assessment of those risks are compiled and communicated to management. Appropriate actions are taken to avoid, accept, transfer, or reduce those security risks based on the potential impact to the business and the likelihood of occurrence.

Penetration testing

Twilio performs penetration tests internally as well as externally by engaging leading security vendors across the globe. Twilio engages independent third parties to conduct application-level penetration tests on an annual basis, to meet compliance obligations. Results of penetration tests are prioritized, triaged by Twilio's Trust & Security team and remediated promptly in partnership with Twilio's R&D teams.

Customers are not permitted to perform penetration testing or scans against Twilio systems. Instead, they may participate in our public bug bounty program abiding by the rules of engagement.

Incident response

Response to security incidents is a critical component of business continuity, risk management, the maintenance and management of the security infrastructure, and in some cases, compliance with laws and contractual obligations. The fundamental tenet of security incident response/handling is an immediate, effective response with minimal impact to confidentiality, integrity, or availability.

Twilio maintains a security incident management program and policies based on NIST SP 800-61 guidance to enable the effective management of security incidents. The Twilio Security Incident Response Team (SIRT) assesses the threat of all relevant vulnerabilities or security incidents and establishes remediation and mitigation actions. The program includes procedures for:

- Preparation
- Detection and analysis
- Containment
- Eradication
- Recovery
- Post-incident activities

Twilio's SIRT is responsible for managing and coordinating activities during a security incident. The team uses information gathered from the evaluation of past security incidents to help identify recurring themes or high-impact threats.

Customer incident notification

Twilio maintains an incident reporting policy that defines conditions under which security incidents are responded to and reported, including levels of severity and risk for various types of vulnerabilities. SIRT receives alerts from upstream vendors and is capable of responding 24x7. The team assesses the threat of all relevant vulnerabilities and establishes remediation actions and timelines for all events.

Twilio notifies customers of an incident by sending an email to an account's specified security contact in the Twilio console. See Twilio data protection addendum for additional details.

DDoS prevention
Twilio leverages industry leading platforms and SIRT to detect, mitigate, and prevent DDoS attacks. Twilio uses AWS Shield Advanced for DDoS protection. Additionally, Twilio has predefined incident alerts set throughout the platform, and testing is performed during annual penetration tests. Our infrastructure incorporates multiple DDoS mitigation techniques in addition to maintaining multiple backbone connections. We work closely with our providers to quickly respond to events and enable advanced DDoS mitigation controls when needed.

Intrusion detection system
Twilio employs GuardDuty, a network-based intrusion detection system (IDS) provided by Amazon Web Services, to analyze AWS CloudTrail, VPC Flow Logs, and AWS DNS logs. The service is optimized for near real-time processing of security detections, using threat intelligence feeds such as lists of malicious IPs and domains, and machine learning to identify unexpected and potentially unauthorized and malicious activity within the Twilio AWS environment.

Threat intelligence
The goal of the Threat Intelligence program is to understand and proactively manage external threats to Twilio's assets, data, people, and systems. The team's core objectives are to:

- Obtain and maintain comprehensive visibility of threat actors and threat actor tactics, techniques, and procedures posing a threat to Twilio
- Provide actionable cyber threat intelligence reports to internal Twilio stakeholders to continuously improve Twilio's security posture
- Build information sharing relationships with external partners

Insider risk
Twilio's Insider Risk Program executes several strategic initiatives designed to deter, detect, and mitigate insider threats to Twilio's people and resources. These initiatives establish a framework for protecting Twilio's workforce and safeguarding our sensitive information:

- User activity monitoring (UAM)—this capability, deployed across all endpoints throughout the enterprise, works with other efforts to detect internal threats to Twilio endpoints and reduce the risks to sensitive information. In addition, this program helps set and enforce policies for properly protecting, interpreting, storing, and limiting the access to UAM methods and results to authorized personnel.
- Partnerships among internal stakeholders—the Insider Risk Program maintains strong internal partnerships to deter, detect, and mitigate insider risk, bridging the gaps between teams to establish a shared vision. The program engages stakeholders on mutual agreements for information sharing, and standardized, repeatable processes for deterring, detecting, and mitigating insider threats.
- Analysis and response—this initiative maintains an insider threat analytic and response capability to gather, integrate, review, assess, and mitigate anomalous information derived from multiple sources. The Program works to mitigate insider risks through referral or response, in order to protect Twilio's people and resources.
- Workforce education—this initiative helps to build a culture of knowledge and individual responsibility to help harden Twilio against insider risk. The program builds the culture through recurring

training and education, including the importance of identifying possible threats; how to identify high-risk behavior; and how to share concerns. One goal of the Program is to develop a team of insider risk professionals, leveraging existing industry training.

- Program oversight and employee privacy—the Insider Risk Program has established oversight mechanisms and procedures to ensure proper handling and use of records and data, restricting access to insider risk personnel who require the information to perform authorized functions.

Twilio's Chief Security Officer oversees the program directly. Annually, or as required by Twilio policy, the Legal department conducts oversight review to ensure compliance with applicable laws, policies, and standards to ensure all legal and privacy issues are appropriately addressed for each part of the Program.

Operational resilience

Twilio takes measures to protect customers and their services through our high-availability platform architecture, resiliency practices and requirements built into our development and operational processes. We maintain Business Continuity, Disaster Recovery, and Crisis Management programs staffed with industry experts who have helped scale similar programs for Fortune 500 companies, with a focus on regulatory compliance frameworks and cloud service architecture.

Business continuity

Twilio ensures continued delivery of our products and services by following an annual program cadence of core activities ranging from business impact analysis to plan development and testing. Twilio performs an annual business impact analysis (BIA) to understand business requirements, set recovery objectives, and identify gaps and areas of vulnerability. The requirements and objectives set during the BIA inform the strategy analysis and Business Continuity Plans (BCPS) which are tested annually. Risks identified during the BIA are included in the Trust & Security's risk management processes. BIAs are reviewed, updated, and approved annually by leadership, or as significant organizational changes occur.

Disaster recovery

Twilio's Disaster Recovery (DR) Program establishes a framework to support its critical business functions to an acceptable level within a predetermined period of time following a disruption. Twilio infrastructure uses a variety of tools and mechanisms to achieve high availability and resiliency. Twilio provides customer-facing copies of DR Test Reports, when available, to customers who have current non-disclosure agreements (NDAs) in place.

Backups
Twilio performs daily backups of Twilio account information, call records, call recordings, and other critical data using Amazon S3 cloud storage. Backups are encrypted in transit and at rest using strong encryption (volume level, AES - 256) and stored redundantly across multiple US availability zones and regions in AWS S3 buckets (cloud). Backup data is kept for one year.

Redundancy
Twilio maintains redundant inbound and outbound connectivity with multiple network carriers and real-time systems to dynamically route

each call or message via the carrier with the most reliable connectivity at any time, responding automatically to carrier availability and reliability, in addition to operating Twilio services across several AWS Availability Zones within the US-East region.

Crisis management

The mission of the Crisis Management program at Twilio is to avert potential crisis events and manage those that occur. This is accomplished by preparing response and recovery plans for a wide range of high-impact adverse events, such as a major cybersecurity event, severe product failures, or safety and security issues affecting a large portion of Twilions.

Read more about operational resilience at Twilio.

Physical security

The Corporate Security Operations team manages functions within the company that are responsible for facility security, physical security, travel security, employee protection, and threat response and intelligence. Twilio headquarters and office spaces are protected by 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.

Twilio's production infrastructure is housed primarily in Amazon Web Services (AWS) data centers, which are secured by professional security staff as well as a variety of physical controls at the perimeter and building ingress points. AWS data centers are geographically diverse, with independent power grids and redundant power, HVAC and fire suppression systems. The AWS data centers use state-of-the-art practices for fault tolerance at each level of the system infrastructure, including Internet connectivity, power and cooling. Additional details on the physical security services provided by Amazon Web Services (AWS) are available at AWS Data Centers.

Managing third party security risk

Twilio contracts with third parties to provide a broad range of services ranging from office chairs and advertising to IT software and data center services. Prior to entering into a relationship with third parties (i.e., vendors), Twilio's Third Party Security team reviews the security posture of the vendors by conducting a risk-based security assessment. This assessment identifies security risks and potential threats of connecting to systems and/or sharing sensitive data with a vendor. Security risks identified in the assessment are tracked to remediation. If several high severity security issues are identified for a third party, a security exception must be filed and approved before engaging with the third party for services.

Third party agreements include confidentiality, privacy and security obligations (when applicable) to ensure data vendors may access, store, and/or process maintain an appropriate level of security controls/protection.

Tiering of third parties

Third parties are tiered according to the inherent risk they might pose to Twilio. The program takes into account the types of systems or

data accessed, volume and classification of data in scope, business continuity and disaster recovery concerns, along with legal and regulatory requirements.

Third party monitoring

Twilio periodically conducts security monitoring assessments of existing critical third parties. Monitoring assessments include evaluating whether there have been any changes to the scope of the services provided to Twilio and whether any system outages or breaches have occurred, requesting updated security documentation and obtaining remediation status for any risk issues previously identified.

Third party offboarding

Upon the termination of a contract, the Third-Party Security Risk Management team is notified via the Global Procurement process for off-boarding ensuring all data is securely deleted and/or destroyed, if applicable.

M&A risk management

The purpose of the Mergers & Acquisitions (M&A) Risk Management program is to protect Twilio by identifying and raising cybersecurity risks prior to completing an acquisition. Results from the security due diligence process enable Twilio leadership to make informed decisions on the potential impact of an acquisition, as well as the time and resources required to resolve any issues after the deal closes. The program also manages integration planning efforts where there are potential security implications both for customer facing and internal systems. The program takes a risk-based approach to assess the acquisition target's overall security posture and effectiveness of its security controls to protect against breaches and other cybersecurity threats.

The program facilitates collaboration across multiple cross-functional teams such as the Integration Management Office, Tech Services, R&D, Privacy, and Legal, in three phases:

1. Due diligence: Pre-acquisition security assessment of the target to identify issues and assess the security posture prior to deal signing
2. Integration planning: Pre-integration readiness, gap analysis
3. Post-close integration: People and systems integration into Twilio

Compliance

Twilio maintains and monitors compliance with applicable security frameworks and regulations. On an ongoing basis, Twilio evaluates the need to meet certain legal, regulatory, and contractual information security requirements. Twilio is committed to abiding by contractual terms with its customers and service providers.

Audit findings and remediation activities are documented and retained according to the Twilio Legal Data Retention Policy and/or authorized by Legal. Audit findings are communicated to the appropriate owners, relevant Trust & Security team members, and appropriate Twilio management. Audit findings are placed on a defined remediation program in order to track and achieve resolution. Audit findings found to be high risks to Twilio or customers are addressed with the highest handling priority.

Twilio services certifications and compliance
As part of our information security management system (ISMS), Twilio is certified under ISO/IEC 27001, has attestations to ISO/IEC 27017 and ISO/IEC 27018, and maintains SOC 2 compliance.

ISO/IEC 27001:2013
ISO/IEC 27001 is a globally-recognized, standards-based approach to security that outlines requirements for an organization's information security management system (ISMS). Twilio has considered all sections of the ISO 27001 standard in scope and has no exclusions in the ISO 27001 Statement of Applicability. For all areas of the standard, Twilio has demonstrated adherence to the requirements as validated by our auditors.

ISO/IEC 27017
Conforming to ISO/IEC 27017 demonstrates our commitment to managing security at every level of our organization. Alignment with these globally recognized best practices specific to cloud services strengthens Twilio's ISMS to ensure controls in place are continuing to align with industry best practices.

ISO/IEC 27018
Conforming to ISO/IEC 27018 demonstrates our commitment to protecting our customer's content. Through the implementation of these internationally recognized best practices, Twilio has expanded our ISMS to include controls that are focused on public cloud Personally Identifiable Information (PII).

System and Organization Control (SOC) 2
The SOC 2 reports provide assurance that controls at a service organization relevant to selected criteria are operating as designed, either as of a point in time (Type I) or over a period of time (Type II). Twilio's current SOC 2 Type II reports include the Security and Availability criteria. Twilio maintains SOC 2 Type II compliance for the following services:

- Programmable Voice
- Programmable Video
- Programmable SMS
- Twilio Flex
- Verify
- Lookup
- Twilio Conversations
- Studio
- Twilio Authy
- Twilio SendGrid

CSA STAR Self-Assessment
The Cloud Security Alliance Security, Trust, Assurance, and Risk (STAR) Registry documents the security and privacy controls provided by cloud computing offerings. Twilio has completed the CSA STAR Self-Assessment.

Twilio helps customers comply

As Twilio evolves to serve larger enterprises and customers in highly regulated industries, we recognize the need for elevated security controls and capabilities. This has led to an increased investment in growing our team of security professionals, expanding our technology, and partnering with customers to make sure they can leverage our services securely.

FIPS 140-2 Level 3
Federal Information Processing Standards (FIPS) are applicable across a number of industries, especially the Financial Services vertical. Twilio has deployed the ability for qualifying customers to request their accounts be enabled with technology that meets the FIPS Level 3 compliance requirements.

HIPAA eligibility
The Health Insurance Portability and Accountability Act (HIPAA) was signed into law in 1996 as part of a larger healthcare reform in the US. Part of the legislation is aimed at providing security and data privacy protections around access, use, and disclosure of protected health information (PHI). HIPAA covers any organizations that meet the definition of "covered entities" or "business associates".

Under HIPAA, companies that use a service provider to process PHI on their behalf must put in place a business associate agreement with that service provider. Accordingly, customers that are subject to HIPAA compliance and intend to utilize Twilio's products and services to develop communication workflows containing PHI must execute a Business Associate Addendum (BAA) to Twilio's Terms of Service. Twilio's BAA was developed taking into account the specific products and services that Twilio offers and considers HIPAA compliance as a shared responsibility between the customer and Twilio.

HIPAA supports Twilio's goal of elevating our data privacy and security to meet the needs of our Healthcare and Lifesciences customers. Twilio is committed to providing a platform trusted by qualifying customers and their patients. To support this, Twilio has developed the Architecting for HIPAA on Twilio whitepaper for our customers to use as a resource; this whitepaper is updated as more of Twilio's platform is made HIPAA eligible.

Payment Card Industry Data Security Standard (PCI DSS)
PCI DSS is a proprietary information security standard administered by the Payment Card Industry Security Standards Council (PCI SSC). 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 payment brands and administered by the PCI SSC.

Twilio's Programmable Voice <Pay> service is PCI DSS Level 1 compliant and can be used to collect and tokenize credit card data over the phone and/or optionally make a payment on behalf of customer applications. Twilio does not store cardholder data on our platform. See Twilio's PCI whitepaper and responsibility matrix.

For payments made to Twilio, a third party handles all Twilio's credit card transactions. We are a PCI Level 3 Merchant, which means that we can accept credit cards as a form of payment but credit card numbers do not enter our environment during customer payment for Twilio services.

Data privacy

Twilio strives to maintain the confidentiality, availability, and integrity of our data and services while maintaining compliance with legislative, regulatory, and contractual requirements. To achieve this goal, a set of core security principles is leveraged to guide the creation of this Information Security Policy. From these guiding principles, Twilio builds and maintains the foundations of a strong security posture.

Binding Corporate Rules (BCRs)
BCRs are binding data protection policies that are approved by European data protection authorities after significant consultation

and which enable multinational businesses, such as Twilio, to make intra-organizational transfers of personal data across borders in compliance with EU data protection law. BCRs function as a code of conduct for Twilio's data protection practices, based on strict principles established by EU data protection authorities and the General Data Protection Regulation's (GDPR) standards and requirements.

Twilio's BCRs were approved in May 2018 and demonstrate Twilio group members' commitment to provide adequate protection of personal data throughout the organization, regardless of the group members' location in the world. Twilio's BCRs enable the transfer of personal data to Twilio group members across borders in compliance with EU data protection law. For more information, see Twilio's Binding Corporate Rules.

General Data Protection Regulation (GDPR)
The GDPR is a data protection regulation established in the EU and EEA in May 2018. Over the ensuing years, it has become the global standard for privacy and data protection law. Twilio views the GDPR as an opportunity to build a stronger data protection foundation for the benefit of all. Twilio is committed to ensuring that our platform is GDPR compliant.

For new products, enhancements or material changes in processing, we proactively apply the Data Protection by Design principles. We apply GDPR standards to all data, not just EU personal data. This strategy provides Twilio the agility to maintain compliance with existing, new and revised data protection regulatory frameworks around the world. For more information, see Twilio & the General Data Protection Regulation (GDPR).

Government requests for information
Twilio only responds to requests that are sent from a government agency via registered email domain; are issued where Twilio is subject to jurisdiction; have an enforceable subpoena, court order, search warrant, or equivalent legal process, compel us to produce the information requested; and states the categories of records sought and specific time period. To learn more about how Twilio Submits to Law Enforcement Requests, check out this page.

Check here for a complete product compliance list.

Note: In July 2020, the European Court of Justice (ECJ) invalidated the EU-U.S. Privacy Shield with the *Schrems I* and *Schrems II* rulings. The U.S. government disputes the merits of the ECJ's ruling, but an alternative has not been proposed.

AWS certifications
Twilio leverages AWS data centers, trusted to be highly scalable, secure, and reliable. Information about AWS audit certifications is available on the AWS Security website and AWS Compliance website.

Shared responsibility

Twilio acknowledges that security is a shared responsibility between Twilio, our partners, and our customers. To remain resilient against future threats, we must always be evolving together.

Twilio's responsibility
Twilio is responsible for our APIs, our products and services, and our customer and partner data. The Twilio Security Overview incorporated into and made a part of (a) Twilio's Terms of Service; (b) the Twilio Platform Agreement; or (c) a similar written agreement between Twilio and Customer for Customer's use of the Services 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.

Our APIs
We're responsible for faithfully executing API calls your app makes, securely and in accordance with our documentation. It's up to us to provide you information sufficient for you to determine whether you can use Twilio in a compliant manner.

Identity and access management
Twilio is responsible for securing our own systems, including determining appropriate levels of privilege across our organization and infrastructure, and for ensuring that our APIs are secured. 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 as part of their job function and requires approval, strong multi-factor authentication, and access via a bastion host.

Information security
Twilio supports encryption to protect communications between Twilio and your application. We also take steps to protect your account information, including call records. Twilio secures your digital authentication credential secrets using industry best practice methods to salt and repeatedly hash your credentials before they are stored. Users can add another layer of security to their account by using two-factor authentication (2FA) for the Twilio console. Twilio performs regular backups of Twilio account information, call records, call recordings and other critical data using Amazon S3 cloud storage. Backups are encrypted in transit and at rest using strong encryption. Backup files are stored redundantly across multiple availability zones in U.S data centers and are encrypted.

Your responsibility

As a partner or customer, you are responsible for ensuring your compliance with applicable laws and regulations, and for protecting your customers' data. You are always responsible for the security of anything under your direct control.

Compliance
When it comes to compliance with regulations and laws, you are responsible for ensuring that it is possible for you to use Twilio in a compliant manner, and that your software applications' instructions to Twilio comply with applicable law.

Your application
It's your responsibility to secure your code throughout the entire software development lifecycle, including protecting your repositories, testing the application throughout the process, and securing production systems and any other connected systems or networks. You, our customer and the builder of the software application, are responsible for implementing and maintaining appropriate configuration properties for the Twilio products, services, or API you use and for the instructions your software application sends to Twilio. You must protect your API key, auth token or other credentials from unauthorized access, and must never hard code credentials in your app or push them to your repository.

Identity and access management
You are responsible for your identity and access management controls, including determining appropriate levels of privilege across your organization. It's your responsibility to create and maintain authentication and authorization systems, including all mechanisms needed to secure them properly.

Information security
You are in charge of the security of your information and your customers' data, including how it is accessed, processed, and stored.

Network security
You are responsible for your network, including any connection points to the cloud or other networks. It's up to you to secure your on-premises infrastructure, employee or user devices, and any applications that run on these devices or infrastructure. Best practice is to set up monitoring and alerting to help you detect and respond to any potential incidents or threats.

Learn even more about our security program

- Twilio Trust & Security
- Operational resilience at Twilio
- Twilio & HIPAA
- Twilio & PCI DSS
- Twilio & GDPR
- Twilio's Binding Corporate Rules (BCR)
- Anti-fraud developer's guide

About Twilio

Millions of developers around the world have used Twilio to unlock the magic of communications to improve any human experience. Twilio has democratized communications channels like voice, text, chat, video, and email by virtualizing the world's communications infrastructure through APIs that are simple enough for any developer to use, yet robust enough to power the world's most demanding applications. By making communications a part of every software developer's toolkit, Twilio is enabling innovators across every industry—from emerging leaders to the world's largest organizations—to reinvent how companies engage with their customers.

Do you need more information? Talk to an expert.

Millions of software developers use Twilio's platform and communication APIs to help businesses build more meaningful relationships with their customers.