8x8

Version 3.0, March 2026

8x8 Communication APIs

Security Overview

8x8

Table of Contents

8x8

8x8

Security Is Our Top Priority

The 8x8 Communication APIs platform empowers businesses all over the world to reimagine workflows, increase adaptability to change, and transform customer experiences through automated notifications, engaging marketing campaigns, efficient customer support operations, and security authentications. But for our customers to integrate our SMS, voice, video, and chat apps capabilities with peace of mind, 8x8 first and foremost ensures that the platform is absolutely secure, private, and reliable.

We know that security is of vital importance to you, which is why 8x8 protects your business using the highest levels of data security, privacy, and compliance - verified by third-party security and compliance certifications. This document will give you a better understanding of 8x8's security best practices and how we safeguard our customer information.

8x8

Comprehensive Processes That Meet the Highest Security Requirements

At 8x8, we are dedicated to empowering our customers with solutions that will not only enhance their customer engagement, but will also protect them and their own customers against any security risks. We strive to maintain the integrity, availability, and confidentiality of the 8x8 Communication APIs platform with a combination of:

1. Documented policies and procedures
2. Management oversight
3. Security-first and privacy-first cultures
4. Technology implementations using security-by-design principles

These management practices are implemented in all areas to protect our systems, data, and personnel, as well as to ensure compliance with industry best practices and standards.

1. Policies

8x8 maintains processes for reviewing and updating policies. Our Human Resources (HR) and Engineering teams review policies to ensure accuracy and validity to current operations. Our HR team is responsible for initiating reviews of personnel related policies, while our Engineering team covers policies relevant to product development and ongoing operations. All policies are available for reviews, which are conducted at frequent intervals.

2. 8x8 security program framework

We implement a security program framework, which defines security measures to protect 8x8, customer data, and 8x8 physical and information assets from internal, external, deliberate, or accidental threats.

The 8x8 security program establishes a structured approach to develop, implement, and maintain appropriate security levels of physical and information-related risk. This program entails ongoing activities to establish and maintain relevant policies and procedures, technology, risk mitigations, training, and awareness.

8x8

8x8's Security Organization

At 8x8, we deliver a trusted platform where all sensitive data is processed with reliability and security. Achieving internationally recognized certifications demonstrates our commitment to the protection of all user data.

1. Compliance programs

8x8 takes the lead in the cloud-based communications industry for data security across a company's entire enterprise.

We maintain externally validated support for data security regulations and standards, including SOC 2 Type II, FISMA/NIST, HIPAA, and PCI-DSS.

SOC 2 Type II compliance

System and Organization Controls (SOC) is a suite of audit reports defined by the American Institute of Certified Public Accountants (AICPA). It is intended for use by service organizations to validate internal controls over their information systems and issue compliance reports to the users of their services.

8x8 SOC 2 compliance is audited by a nationally recognized Qualified Security Assessor (QSA) to ensure effective control implementation over a defined audit period.

FISMA / NIST 800-53 R5 guidelines

NIST Special Publication 800-53 is a catalog of security and privacy controls intended to assist federal agencies and corporations that implement the Federal Information Security Modernization Act of 2014 (FISMA) to protect their data and information systems.

A nationally recognized Qualified Security Assessor (QSA) performed an assessment of the 8x8 environment and found 8x8 to be NIST SP 800-53 R5 compliant at the FISMA Moderate level.

HIPAA Security Rule compliance

The Health Insurance Portability and Accountability Act (HIPAA) stipulates how Personally Identifiable Information (PII) maintained by the healthcare and health insurance industries should be protected from fraud and theft.

8x8's third-party auditing organization, A-Lign, assessed our controls for SOC 2 Type 2 compliance and they completed an in-depth mapping to HIPAA requirements for our entire product offering. The mapping demonstrates proper controls between our SOC and HIPAA requirements. A-Ligns' auditors have validated that our environment does protect HIPAA data.

CSA Cyber Trust compliance

The Cyber Trust mark is a cybersecurity certification for enterprises with more extensive digitalised business operations. It serves as a mark of distinction for enterprises to prove that they have put in place good cybersecurity practices and measures that are commensurate with their cybersecurity risk profile.

8x8 Cyber Trust compliance at the Advocate Tier is certified by independent third-party audit firm TÜV Süd.

ISO 27001 compliance

ISO 27001 is an international standard framework for an effective Information Security Management System (ISMS). ISO 27001 requires that management systematically examine the organization's information security risks, design and implement a coherent and comprehensive suite of information security controls and adopt an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis.

8x8 has been found to be compliant with the requirements of ISO 27001:2022, incorporating the additional ISO 27017:2015 and ISO 27018:2019 controls by an accredited certification body following successful completion of an audit.

PCI-DSS 4.0 compliance

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card schemes/providers.

8x8's services have been reviewed by a nationally recognized Qualified Security Assessor (QSA) and have been assessed PCI compliant.

View 8x8's Security and Compliance certifications

2. Industry-leading security and compliance

We believe that any enterprise product or service must meet or exceed existing customer security and compliance requirements. From the beginning, 8x8 has prioritized security and compliance certifications to meet the needs of companies in all industries. Because of this focus, 8x8 solutions have been selected by both national and multinational organizations to help them comply with strict standards, protect their reputations, and secure their customer data.

At 8x8, security starts with the actual software driving all cloud solutions that we provide. Prior to launch, all service offerings go through rigorous software code security stress testing using static and dynamic analysis.

3. 8x8 security experts

Ensuring that security is represented and executed at the highest levels of the organization, 8x8 appointed a Chief Information Security Officer (CISO) who brings over 20 years of cybersecurity and information technology leadership experience to 8x8 in the areas of data privacy, intellectual property protection, risk management, and corporate cyber governance. The CISO's team includes certified security professionals with 10 or more years of dedicated security and compliance experience.

The team holds information security qualifications & certifications, such as:

- Certified Information Systems Security Professional
- Certified Information Security Manager
- Certified in Risk and Information Systems Control
- Lead Auditor in ISO 9001:2015 Quality Management Systems
- Lead Auditor in ISO 27001:2013 Information Security Management Systems
- Offensive Security Certified Professional

8x8

- Offensive Security Web Expert

8x8

Hacker-powered Security Programs

8x8's Responsible Disclosure & Bug Bounty programs

8x8 runs responsible disclosure and incentivized bounty programs through HackerOne to allow anyone to report vulnerabilities. With this NIST best-practice RDP, we have a well-defined process for finding and fixing vulnerabilities - before they can be exploited. By partnering with the global hacker community, we keep our customer and partner data safe and secure.

View the 8x8 Responsible Disclosure program

8x8

8x8's Personnel Security

At 8x8, we foster a strong security culture to build security consciousness in all our employees. We strive to reinforce the importance of safeguarding the company, our customers, and all data through our security policies, codes of conduct, and shared mission. At the same time, we empower our teams to do so by providing them with the necessary training, tools, and knowledge.

8x8's organizational structure provides the framework within which activities for achieving objectives across its corporate structure are planned, executed, controlled, and monitored. 8x8's management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility and appropriate lines of reporting. This organizational and corporate structure is based, in part, on its size, geographical scope, and the nature of its activities.

1. Management communications

8x8's management philosophy is founded on clear communication of the organization's tone, direction, and expectations. Leadership communicates the tone and direction of the organization to individual team members through policies, meetings, newsletters, emails, and the 8x8 Employee Handbook.

The Employee Handbook includes Standards of Conduct and addresses disciplinary actions, including termination, that could result from failing to comply with these standards. 8x8 has established hiring procedures to onboard its new employees securely and consistently. All new hires receive the handbook as part of their onboarding and must acknowledge their understanding of the included policies. The handbook is maintained in a location that is accessible by all personnel. Additionally, we have published and distributed a privacy manual to communicate requirements for compliance with privacy legislation.

2. Security trainings

8x8 deploys a comprehensive training program for new starters and annual refreshers for all those with access to 8x8 systems. Employees are required to complete mandatory training that covers all areas of Information Security including Social Engineering, Privacy and Compliance with legal requirements. The training is enforced through regular testing.

Role specific training defined by the job role is subsequently provided where processes

to enforce policies are shared. The more pertinent policies, including; HR Policies, IT Systems, Privacy and Security are detailed to all staff and are included in annual refreshers. 8x8 utilizes online training platforms which record completion and scores for management and compliance purposes. Responsibility for ensuring attendance and completion to the mandatory training is the responsibility of managers.

We provide security awareness training and job-specific training to employees at least annually to ensure that they are adequately prepared to perform their assigned information security-related duties and responsibilities.

3. Background checks

8x8's Background Checks Guidelines require all new employees to undergo a standard background check consistent with local laws, including in foreign countries where 8x8 operates, and additional checks are completed based on job roles and regulations. We conduct background checks, including financial, education, employment, and criminal history reviews, for all new staff before they start, with additional in-depth checks for staff who require access to more sensitive data or systems. The information obtained through background checks is confidential and will be shared only with individuals for essential business reasons.

4. Building cybersecurity awareness

8x8's security team deploys randomized real-life anti-phishing campaigns and conducts mandatory security awareness training to the entire organization. In addition, specific and targeted training is assigned to all relevant teams. This includes developers who go through an annual training on Open Web Application Security Project (OWASP) security basics and the latest trends in secure software development, to ensure that they are aware of the most current vulnerabilities.

5. 8x8 Ethics and Compliance helpline

8x8 has implemented a helpline that enables employees to report an incident about workplace issues, such as financial and auditing concerns, harassment, theft, substance abuse, and unsafe conditions. We take all reports of a violation or fraudulent auditing and accounting activity very seriously and ensure that they are promptly and thoroughly investigated.

8x8

8x8 Communication APIs : Secure by Design

We developed 8x8 Communication APIs with security best practices and a Security by Design approach at all times. By proactively identifying, mitigating, and protecting against security threats from start to finish, we ensure that communications between 8x8 and customer applications are secure and free of security vulnerabilities.

1. Application development

The application suite of 8x8's Communication APIs platform is developed and maintained by our in-house developers and operations personnel. The roles and responsibilities of these teams are defined and appropriately divided to ensure segregation of duties. Separate system components are used for production and non-production environments, and access to these environments is limited based on job requirements. We are leveraging separate AWS accounts and Google projects, utilising separate Virtual Private Cloud (VPC) networks and Kubernetes clusters, and are deploying them on separate technology stacks, as appropriate for the application's deployment methods.

2. Secure Software Development Life Cycle

Secure Software Development Life Cycle (SSDLC) Policies and Procedures define the processes that support the approval, planning, and lifecycle development of 8x8 information systems.

During the initial design, security is evaluated in terms of the overall functional design specification, and the information processed by the application is classified in accordance with the Data Classification Standard.

Developing the 8x8 Communication APIs platform, our SSDLC includes multiple stages of review, starting with an architectural review at the beginning of new projects, ongoing code checking by manual peer review, further review by security staff, and automated reviews utilizing static application security testing (SAST) and dynamic application security testing (DAST) tools.

8x8 provides initial and ongoing training to ensure that employees practice secure coding.

- Code scanning tools are used to scan all 8x8 repositories. Code repository access is managed at the individual developer level with groups defined for products and roles. Authentication is configured for two-step verification, and versioning is enabled.
- We review all software from external sources, such as outsourced code, for security implications.

Our engineering departments practice a “Shift Left” security culture to find and prevent defects early in the software delivery process. We engage certified security vendors to conduct penetration tests of our external facing surface. Throughout the year, security researchers are continuously testing products and infrastructure through the 8x8 Responsible Disclosure & Bug Bounty programs.

3. Data retention and classification

We retain data only as required to satisfy business, legal, and regulatory requirements. We have a data classification program in place to identify and provide reasonable protections to confidential information.

8x8 established data classification procedures in accordance with GDPR, HIPAA, Title 18 of the U.S. Code, The Privacy Act of 1974, and Standard Contractual Clauses (SCC). The Data Classification Standard requires data to be classified as restricted, confidential, or public. Restricted data is limited to certain people and an access granting policy is in place. Confidential data is highly sensitive and is protected by statutes, regulations, policies, and/or contracts. All customer data is considered Restricted.

4. Change management

Change management drives the successful adoption and usage of change within the business. 8x8 has created defined configuration standards that ensure all configuration, maintenance, diagnostic, development, and repair activities are managed and monitored to preserve the confidentiality, integrity, and availability of 8x8’s information system resources. 8x8 adheres to the following change control policies and procedures:

- A ticketing system is used for all change requests, and the process for implementing a change is tracked on its ticket.
- Testing plans are developed to determine the success/failure of the change and backout plans are developed in the event of unsuccessful changes.
- Changes are deployed to staging environments first, and only after successful test cases are considered for a production deployment.
- All configuration standards are based on CIS benchmarks.

We ensure that all changes are subjected to peer review and approved prior to implementation.

5. Secure standards

8x8 protects customer information using the following approaches to support secure standards:

- Transport Layer Security (TLS) version 1.2 is used to encrypt data in transit.
- Short Message Peer-to-Peer (SMPP) protocol via TLS is used as supported by the carriers, and the SMPP interface is protected by defined whitelists.
- 256-bit AES algorithm in Galois Counter Mode (AES-GCM) is used to encrypt data at rest.
- Sensitive information (such as API keys) are additionally encrypted using column-based encryption within the database(s).
- Strong encryption parameters are used for remote user access.

6. Built-in security

8x8 proactively provides application security and authentication to all our users by building security right into our software:

- Number Lookup API: Cleans user database and steps up on anti-fraud measures by checking the validity of phone numbers and their current locations.
- Mobile Verification API: Generates and authenticates SMS-based or phone call-based mobile verification requests.
- Number Masking API: Enables users to connect to a phone call while keeping their phone numbers private.
- Remove Personally Identifiable Information (PII) API: Removes PII for particular messages from 8x8 databases.

The 8x8 Connect customer portal secures user authentication with:

- Two-Factor Authentication (2FA): Achieved via an Authenticator app or SMS Verification (OTP) and can be enforced for all users
- Single sign-on support via SAML identity providers such as Okta, Google, Azure Active Directory, JumpCloud, etc
- Password complexity rules: Minimum 8 characters in length, must contain at least 1 alpha character, must contain at least 1 numeric character, utilizing open source password strength estimator
- Logout after idle time duration: Session limit is customizable
- Password expiration: Mandatory password rotation every 180 days
- Forced logout once a user gets deactivated/removed

8x8

8x8's Infrastructure Security

8x8 invests in infrastructure safeguards that restricts access to our cloud, data, and platform networks, implementing multiple layers of security, including physical, network, system, and application security protocol.

1. Cloud security

8x8 ensures that tight security controls are in place on our infrastructure.

- The 8x8 Communication APIs platform uses trusted cloud providers, such as Amazon Web Services (AWS) and Google Cloud Platform (GCP), for cloud computing.
- To set up a secure architecture, we utilize virtual private clouds (VPCs), subnets, security groups, and threat detection.
- We implement segregation between development, quality assurance (QA), and production environments, as well as between voice, video, and messaging/SMS product environments.

The 8x8 Communication APIs platform utilizes several security products across multiple cloud platforms for the best customer experience and defense:

- All inbound network access is restricted on a whitelist basis to only allow authorized access.
- Intelligent Threat Detection (such as Amazon GuardDuty) ensures continuous monitoring of network traffic.
- Data Security and Privacy Services (such as Amazon Macie) help protect sensitive data in AWS.

2. IT equipment security

8x8's IT landscape is secured using the following measures:

- CIS standards are followed for workstation hardening.
- Configuration management and hardening is enforced through Mobile Device Management Software (MDM).
- MDM solutions manage Antivirus deployments and OS Patching.
- Endpoint Security Threat Prevention prevents threats from accessing systems and runs targeted scans for malware on workstations.
- Windows Devices & Mac devices utilize hard disk encryptions.
- Devices are cycled out in alignment with their warranty.

- MFA is required for all remote access to production systems, and all access to centrally managed production network environments requires MFA-protected VPN access.
- 8x8 has implemented Data Loss Prevention (DLP) tools to detect and alert on suspected security issues relating to the loss of data, as well as using and expanding the use of DLP functionality in several of our other control tools.

3. Industry best practices

8x8 utilizes benchmarks created by the Center for Internet Security (CIS) to harden any target system based on best practices for secure configuration. CIS Benchmarks are the only consensus-based, best-practice security configuration guidelines both developed and accepted by government, business, industry, and academia. The Information Security Team approves system configurations prior to implementation.

4. System account management

8x8 maintains policies and procedures that address how employee access requests and accounts are managed. Access is assigned to personnel based on the principle of least privilege and need-to-know. Prior to granting access, the data owner must approve the request.

Internal and external systems are connected to a single sign-on solution which enforces password complexity rules and multi-factor authentication. We utilize Zero Trust Network Access (ZTNA) to remove application assets from public networks and significantly reduce the surface area for attacks.

8x8

Monitoring and Vulnerability Management

At 8x8, we believe that vulnerability management is a fundamental part of good security hygiene, which is why we are dedicated to mitigating the risk of security vulnerabilities, as well as assessing new and emerging security threats. This bolsters our overall security strength and reduces the impact of vulnerability exploitation.

1. Finding vulnerabilities

8x8 maintains a formal risk assessment methodology that documents the process for identifying and evaluating security vulnerabilities affecting confidentiality, integrity, and availability. The assessment is based on NIST SP 800-30, and the process is performed annually and/or following significant changes to the environment.

We implement incident response policies and procedures to define incident identification, reporting, containment, and remediation processes:

- We scan our internal infrastructure at least weekly with vulnerability scanners and internal pentesting tools to identify vulnerabilities.
- Our external attack surface is scanned by an external attack surface management solution.
- Container scanning is used to scan container images in known, registered image repositories or by connecting directly to Kubernetes API servers to acquire running images.
- Cloud Scanning is used to test known Amazon Web Services accounts against the Center for Internet Security AWS Benchmark.
- We utilize external penetration testing and API testing services to identify potential vulnerabilities within our infrastructure and applications.
- Along with internal measures, 8x8 runs Responsible Disclosure & Bug Bounty programs to allow anyone to report vulnerabilities.

Remediation efforts are prioritized using a layered approach. We review each identified issue and, depending on its severity, we deploy a patch within a specified timeframe.

2. Monitoring tools

8x8 has established multiple means of monitoring the security, availability, and confidentiality of its systems:

- Intelligent Threat Detection (such as Amazon GuardDuty) ensures continuous monitoring of network traffic.
- Monitoring/logging and automated responses are implemented based on AWS Security Hub, AWS Config, AWS CloudTrail, AWS CloudWatch, Google Security Command Center, and Google Stackdriver.
- We utilize a host-based intrusion detection solution (HIDS) to actively monitor for intrusions.
- 8x8's Incident Response team monitors all log data for anomalies, utilizing a number of automated scanning tools along with manual investigation of unrecognized or suspicious entries.
- User actions in 8x8 Connect are recorded.

3. Incident Response

8x8 has developed and implemented a formal incident response process for identifying, reporting, containing, and eradicating incidents and breaches. The 8x8 Monitoring Incident Response Standard outlines the roles and responsibilities of the organization's workforce, the Security Team, and the 8x8 Network Operations Center (NOC). This standard includes the coordination of security incidents among business associates; if a breach or potential breach of PHI or PII were to occur, the Chief Privacy Officer would be notified.

The 8x8 Security team is responsible for monitoring security threats, both digital and physical. The Security team must establish and maintain roles, systems, applications, policies, and procedures to mitigate threats while ensuring a quick, effective, and orderly response to security incidents.

8x8

Risk Management

8x8 has a formal, documented Risk Register. The risk management process is in place to identify the organization's critical assets that require protection, and to understand and document risks from security failures that may cause loss of confidentiality, integrity, or availability.

Risk management provides guidance for the analysis of risks and how they should be handled, and is used to determine the appropriateness of selecting controls that transfer, avoid, and mitigate risk. The information security team evaluates risks to drive weekly conversations between the team, including the CISO, where mitigating controls are also developed. A risk register is actively maintained and includes relevant information about each individual risk, including the name of the person who submitted the risk, the affected assets and the type of risk.The risk register then computes the risk priority and allows 8x8 to manage risk based on priority. Action and mitigation plans are also created, maintained and followed through to completion within the risk register.

8x8

Physical Security

8x8 invests in industry standard access controls and physical security measures to ensure a robust security posture.

1. Security in 8x8 office locations

8x8 maintains the security of our offices in a number of ways:

- Offices are equipped with security cameras, access controls, and security guards.
- The server room holds network equipment for the office and requires privileged badge access.
- 8x8 maintains a visitor log to track visitor access into the facility. No visitor access is allowed beyond the lobby level without authorization. Visitors must be pre-authorized with the building security staff and present a government-issued photo ID at the security desk. The office uses a visitor log system which places an electronic date and timestamp, and it records the name, email address, company, and onsite contact for each visitor.
- We have a process for securely destroying confidential media when no longer in use.

2. Data center security

The 8x8 Communication APIs platform leverages different cloud providers, depending on regions and requirements:

- Amazon Web Services (AWS) data centers are secure by design and follow a large set of industry-wide standards. For more information on AWS data center physical security protocols, see the AWS Data Center Controls.
- Google designs and builds its own data centers, which incorporate multiple layers of physical security protections and undergo independent verification of security, privacy, and compliance controls, achieving certifications against global standards. For more information on Google Cloud data center physical security protocols, see the Google Infrastructure Security Design Overview whitepaper.

8x8

Business Continuity and Disaster Recovery

8x8 maintains business continuity and disaster recovery plans, which are used to outline the recovery from significant disruption to critical services. This ensures our operational resilience, enabling the recovery of vital infrastructure to the widest extent possible so that our customers are impacted in the least possible way.

1. Planning

Our systems are categorized into tiers, and disaster response activities are activated based on a tier. 8x8 regularly conducts failover and recoverability testing on critical systems. Recovery Point Objective (RPO) and Recovery Time Objective (RTO) are defined through business impact analyses and recovery procedures are documented. Procedures for how to be resilient during pandemics are included.

Hosting the 8x8 Communication APIs platform on cloud providers allows us to benefit from high availability and resilience against node failures, entire data center failures, and natural disasters.

2. Backups and retention

8x8 performs regular backups of all data necessary to provide the service, as well as all customer data and other critical data using cloud storage. Backup files are encrypted in transit and at rest using strong encryption technologies, such as the 256-bit AES algorithm in Galois Counter Mode (AES-GCM).

8x8 retains the SMS/message and phone call history for six months.

8x8

Third-Party Security

8x8 works with third parties for a range of services from office equipment to data center services. As part of due diligence procedures, we select and retain only vendors that will implement security measures that are consistent with our own security standards. We require vendors to provide evidence of their ability to be compliant:

- Prior to finalizing contracts with third parties, 8x8 attaches the Minimum Third-Party Security Standards exhibit, including the Security & Privacy exhibit addendum, to the agreement.
- The 8x8 Vendor Engagement Process includes a due diligence process including all standard processes, and this establishes that, where necessary, a vendor is able to comply with 8x8's policies and this is incorporated into subsequent contracts.
- Vendors are categorized based on their access to 8x8 data, facilities and networks. This will determine the vendors criticality rating and as well as the type and frequency of reviews conducted.
- 8x8 implements a process for monitoring service providers. Vendor reviews could include but are not limited to, questionnaires, security certification reviews, breach and cyber monitoring

8x8

8x8 Is Committed to Your Security

From 8x8's management approach to our physical, process, employee, product/services, and infrastructure security, as well as business continuity, we have put security measures in place to ensure that our customers' data is secure. To learn more about our security and compliance capabilities, please reach out to cpaas-sales@8x8.com and our Security team can address any specific questions.

8x8

Additional Resources

8x8 Security and Compliance Certifications

Get Started with 8x8 Communication APIs platform

8x8 CPaaS developer portal

SMS APIs:

SMS APIs Developer Documentation

SMS APIs Tutorial

SMS APIs Data Sheet

SMS APIs Customer Case Studies

Messaging Apps:

Chat Apps API Data Sheet

WhatsApp Developer Documentation

Voice APIs:

Voice APIs Developer Documentation

Voice APIs Customer Case Studies

Voice SDK APIs Tutorial

