Dialpad

CLOUD SECURITY OVERVIEW

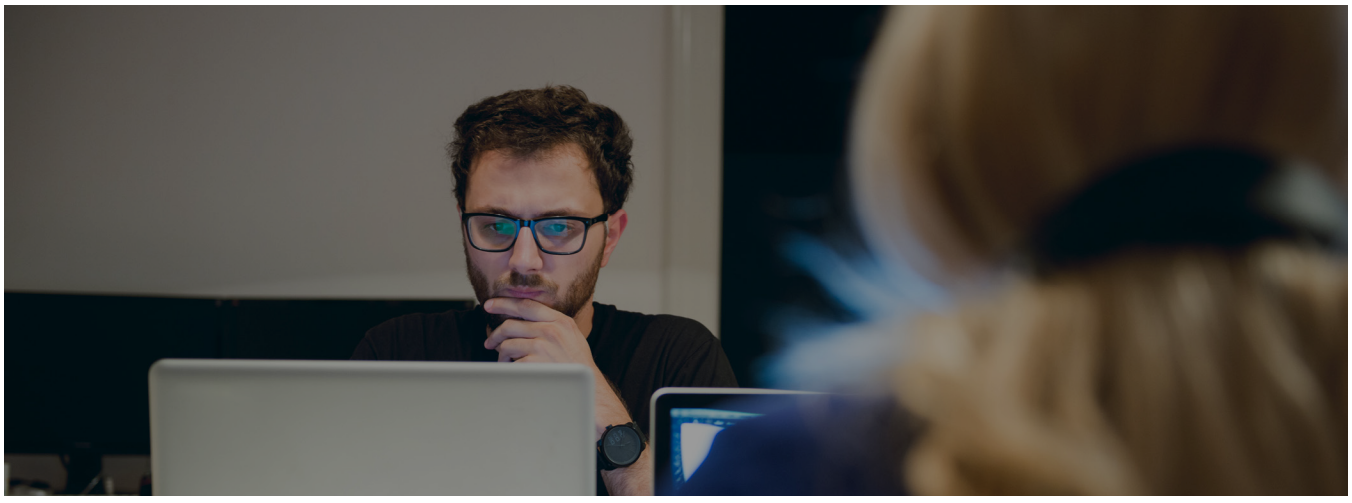
Introduction

At Dialpad, the confidentiality, integrity, and availability of our service is of utmost importance. We understand that your communications are vital to business operations and must be secure and always-available. As a pure-cloud business communications platform, we work hard to ensure security is built into the DNA of our service, freeing customers to take advantage of the innovation, mobility, flexibility, and ease-of-use.

We have taken a comprehensive, multi-layered approach to security, ensuring that every element of your data is secure. And our security policy provides controls at multiple levels of data storage, access, and transfer. Our team is dedicated to making sure that your communications are as secure in our cloud as they would be in any on-premise solution—and often, even more secure than these outdated systems. As a result, thousands of companies use our platform every day.

This document outlines the security program we have in place to ensure the protection of customer information and the availability of our service. Inside, you'll learn about our approach to, and investment in, technologies ensuring:

- Governance
- Physical Security
- Network and Operational Security
- Application Security



Governance

We believe that offering the best security for our customers starts with having a security governance program in place, which includes clearly defined policies, best practices and processes, as well as a team to coordinate and direct the management of our service.

Our security team plays an active role in security governance by proactively auditing and improving security measures and internal processes. Led by Product Management, this team includes representatives from across functional areas, including Security, R&D, customer support, HR, and legal. This dedicated team is in charge of maintaining a security program that covers all operations, services, and systems involving access to confidential customer information. This covers not only the software and infrastructure that runs our service, but also how we hire and train employees, manage our customer accounts, and engage with partners.

PERSONNEL SECURITY

Dialpad conducts background screenings on all employees and staff. We maintain a training program to ensure that relevant staff are familiar with our information security and privacy program. We also have a disciplinary process to enforce internal policy violations.

The security team is responsible for governing our information security and privacy program and ensuring there are policies, processes and procedures in place to identify and address security and privacy incidents. Our incident response plan is available upon request.

PRIVACY AND TRUST

Dialpad has been certified by PrivacyTrust, formerly eTrust, as having met strict privacy and data protection requirements. We have procedures in place that limit access to sensitive information and systems only to necessary staff.

In order to protect the privacy and security of data exposed to relevant outsourcing providers, Dialpad requires that they assert security assurances similar to our own. This is enforced contractually by including security clauses in contracts with our vendors and subcontractors. Dialpad's comprehensive privacy policy is publicly available online, and our internal information security policy is also available upon request.

Physical Security

Dialpad partners with Tier 3/4 Data Center providers that follow physical security best practices. With multiple data center partnerships globally and office locations in numerous countries, Dialpad ensures that all security controls are uniform and compliant.

Dialpad data center physical security capabilities include:

- Two-factor authentication to access all facilities
- Electromechanical locks are controlled by biometric authentication and key-card/badge
- Access to secure sub-areas is allocated on a role-specific basis
- Only authorized data center personnel have access
- Closed-circuit video surveillance, monitored 24x7x365 and data retention for 90 days
- Centralized Security Management Systems to control the Electronic Access Control Systems and COV networks
- Cameras are located on internal and external sides of doors containing access to sensitive areas,
- Sensitive equipment is housed in secure sub areas within the secure perimeter
- Alarms are directly connected to the local Fire and Police Departments
- Data centers are operational and manned 24x7x365 a by a security team and engineering/operations personnel
- Appropriate additional perimeter defensive measures, such as walls, fencing, gates and anti-vehicle controls are in place
- The delivery and loading bays at all Dialpad data centers are separate areas secured by defined procedures and security controls
- Unauthorized visitors are not permitted access to the data centers

Our service is architected to leverage carefully selected third-party platforms and infrastructure, assuring that customer data and the assets storing or processing it are protected against physical tampering, loss, damage, or seizure.

Google Cloud Platform

Our websites, web applications, smartphone backend, and all customer sensitive data is processed and stored using Google Cloud Platform services. The Google Cloud Platform runs on a technology platform that is conceived, designed and built to operate securely. The Google Cloud Platform is [CR2] ISO 27001 certified and Google has completed the SSAE18 / ISAE 3402 Type II (SOC 2 and SOC 3) audit. For more information on Google's approach to security and compliance, please see this white paper.

Proprietary Media Engines

Our telephony engines, which handle call setup and media (i.e. voice or video packet) exchange, are located in numerous Tier 3/4 data centers across the globe. These locations are designed to host mission critical systems and are managed and maintained by providers with years of experience, ensuring that our data centers are secure and reliable.

Some of the safeguards in place include:

- Multiple power grids, full DC battery, redundant UPS (uninterruptible power supply), and dedicated backup diesel generators
- Multi-zoned, high fog, pre-action fire suppression systems
- Dedicated pump rooms and moisture barriers on exterior walls to protect against floods
- Facilities that meet and often exceed local building codes for seismic activity, including use of cabinets that are anchored down in case of an earthquake
- Electronic entry systems that include both key card and biometric access controls
- 24/7/365 manned security
- Windowless exteriors and CCTV inside the entire center, including cage access
- Shipping and receiving sections that are walled off from active server rooms
- Silent alarms and mantrap cages that can be activated under duress

Dialpad's operational status is always available at status.dialpad.com.

Network and Operational Security

At Dialpad, we use multiple layers of network and operational protection to ensure that customer data is adequately protected against tampering and eavesdropping. We implement best practices for protecting the network between our infrastructure and multiple carrier connections across the globe. All critical network infrastructure is locked away, and only select IT-related employees have access.

CHANGE MANAGEMENT

We maintain a change management processes to ensure that all changes to networks, systems, and processes are appropriately reviewed. Our responsible personnel receive automatic vendor mailing lists that inform them about the latest security issues. We have test systems in place where staff can try patches themselves in a non-production environment before patches are deployed in production. We also have a process for installing updates and security patches for operating systems and applications, including an emergency process to install patches outside of the regular patching schedule for security updates that address high-risk vulnerabilities.

FAILOVER AND BACKUPS

Automatic backups are built into our system. This means that if a single server ever fails, another one will take over instantaneously. Should a network connection with a carrier go down, another carrier will pick up the traffic. Should the worst happen (for example, a data center goes offline), calls will be routed automatically through another location. Every aspect of our system has been designed with redundancy in mind so that in the event of a failure, there's always an alternative to take its place immediately.

Every aspect of our system has been designed with redundancy in mind. Our failover methods are extensively documented, reviewed, and continuously tested on a daily basis. In addition, we always have personnel on-call 24/7 to respond to any possible outage.

OTHER TECHNICAL SYSTEMS AND PROCESSES

Dialpad achieves network and operational security through the use of other technical systems and processes such as:

- **Firewalls:** Multiple layers are deployed and monitored to filter and restrict what traffic is allowed into and out of our network
- **Denial-of-Service (DoS) prevention:** To ensure availability of our service, we follow industry-leading DoS prevention practices, including on-premise attack mitigation in our data centers and the use of traffic scrubbing providers
- **Logs and monitoring:** We monitor log access to sensitive information and systems, and have event monitoring in place, complete with staff who are trained to proactively identify unusual activity (i.e., that deviates from normal system and user behavior)

FRAUD PREVENTION

Our team has decades of combined experience building and operating large-scale telephony platforms. Security and fraud prevention were key components of our early design process.

Because we designed our architecture to separate the telephony infrastructure from our application infrastructure, we are able to localize and stop fraud early. Additionally, our analytics and engineering teams regularly collaborate on fraud response, investigation, analysis, and prevention.

Application Security

To ensure application security, Dialpad has deployed several methodologies.

SECURE DEPLOYMENT

We have a source code repository with versioning control so that all source code is checked in. Only engineers with a legitimate need get commit access to the code. Senior engineers review the code to make sure it complies with our stringent requirements, including for necessary security controls and features.

Specific procedures are in place to ensure proper, accurate testing and deployment of applications. For example, in addition to development unit testing, our QA department tests all new functionality and completes full regression testing (both automated and manual) before a new release. This testing is done separately, complementing other comprehensive assessments performed by third-party organizations that test both the application and infrastructure for protection against known vulnerabilities, common penetration techniques, and development pitfalls.

As a final layer of protection, we employ alerts, monitoring, and probes to help detect security issues. If a critical issue somehow makes it into production, we have the ability to easily fall back to the previous version.

STRINGENT CODE UPGRADE PROCEDURES

Before we upgrade our systems with new code, we test continuously via unit tests, functional tests, and end-to-end Quality Assurance regression. New code is pushed to a subset of servers to assure stability before being rolled out globally. When it comes time to deploy new code into production, users notice it silently and flawlessly, by design. We do not have scheduled downtime or maintenance windows, even when upgrading our systems.

We do not have scheduled downtime or maintenance windows, even when upgrading.

DATA ENCRYPTION

Dialpad uses encryption to safeguard customer data both in transit and at rest. All requests to Dialpad services are made exclusively under HTTPS, using TLSv1.1 or TLSv1.2. Our use of Google Cloud Platform ensures customer data at rest is protected using 256-bit Advanced Encryption Standard inside redundant storage at multiple physical locations within the United States. Furthermore, any metadata (user and financial information) and actual data (phone call content) transmitted is authenticated and coded to protect its integrity.

For VoIP calls made through our service (over WebRTC), the signaling for call setup is executed using Websockets and TLS to provide privacy and data integrity. Once the call has begun, a user's voice packets traveling over the internet are encoded in SRTP, or Secure Real Time Protocol. SRTP provides packet encryption, message authentication and integrity, and replay protection so that any sniffed packets are utterly indecipherable. So for VoIP to VoIP calls, such as within your organization, your conversations are actually safer than when they travel over the plain old telephone network.

IDENTITY AND AUTHENTICATION

User authorization of Dialpad services are communicated over HTTPS and are secured with the administrators choice of OAuth2.0, SAML 2.0, or by an email and password combination that is stored encrypted using a secure cryptographic one-way hash function of the salted password.

SEPARATION BETWEEN USERS

The use of Google Cloud Platform enables us to maintain logical per-tenant isolation. Our application ensures both horizontal and vertical access control so that 1) each user's information and data cannot be accessed or impacted by another user and 2) only actions that are appropriate for the role of the currently logged in user are allowed.

SECURE ADMINISTRATION

We believe our customers should be provided with the tools required to help them securely manage their service. We have role-based access and control so that your account administrator can easily:

- Add or remove users and set user privileges
- Set retention policies for voicemail, call, and chat history
- Control use of premium and international calls through prepaid calling credits
- Access a dashboard of aggregated usage statistics and call details
- Additionally, individual users have control over which devices are connected to their account and can remove them at any time.

PENETRATION TESTING

Dialpad environments contracts with a 3rd party security firms annually to conduct Penetration Testing.

Summary

At Dialpad, we promise to be proactive and vigilant in ensuring your data remains safe and secure. Dialpad employs a multi-layered security strategy that supports a cloud-based communications platform used by leading enterprises. We deliver heightened security and availability at no additional cost, saving our customers overhead and expense while providing peace of mind.

For additional questions, please visit us at www.dialpad.com.