SECURITY DATA SHEET

Conga Contracts

Security, privacy, and architecture

Services overview

The Conga Contracts service provides cloud-based contract lifecycle management software to help manage, negotiate and administer all contractual agreements with customers, partners, and suppliers. As a SaaS product, the Conga Contracts service processes and stores customer information in redundant and highly secure data center facilities.

As a Conga Contracts user, you manage all access and usage exclusively through your instance or SAML 2.0 implementation.

Conga infrastructure

The Contracts service is regionally hosted with Amazon Web Services (AWS), available in the continental United States, within Europe, or Australia. Each region is mirrored across multiple, geographically dispersed data centers for fault tolerance and business continuity within the region the service is set to use. Customers may select specific regional processing locations upon implementation or by submitting a support ticket at support.getconga.com/Reference/Contact_Support.

The Conga Contracts service provides clients with secure access to their mission-critical contract management system with a monthly uptime of 99.7%, excluding scheduled maintenance periods as defined within your MSA.

Encryption for external connections

TLS encryption technology is utilized for data transfer between all parties involved in the process. TLS connections are negotiated for at least 256-bit encryption or stronger. The private key used to generate the cipher key is at least 2048 bits. It is recommended that the latest available browsers because they are compatible with higher cipher strengths and have improved security.

Network access control

A limited number of Conga operations team members are granted access to Customer environments, and then only after the completion of a successful background check, awareness and acknowledgment of privacy and confidentiality agreements, and security training. Access occurs through a multi-factor VPN or Private Proxy connection. Additional authentication, authorization, and accounting are implemented through standard security mechanisms. These measures are designed to ensure that only approved operations and support engineers have access to the systems. Remote access to the environment is restricted to select operations staff and only available via two-factor authentication.

Network bandwidth and latency

Conga relies on the AWS network infrastructure to provide low latency network availability between Conga and end users. The AWS Cloud infrastructure is built around regions and availability zones. A region is a physical location in the world where we have multiple availability zones. Availability zones consist of one or more discrete data centers, each with redundant power, networking, and connectivity, and housed in separate facilities. These availability zones offer you the ability to operate production applications and databases which are more highly available, fault tolerant and scalable than would be possible from a single data center. Conga monitors applicable networks and addresses internal issues that may impact availability.

Anti-virus and anti-malware controls

Conga leverages best in class tools in order to monitor and block virus and malware behavior. This includes protection against emerging threats beyond traditional, signature based solutions.

Firewalls and intrusion prevention

Conga utilizes firewalls as one component of a layered approach to application infrastructure security. To control access and allow only authorized traffic to Conga infrastructure, managed firewalls are used. In addition, Conga employs security policies to manage ingress and egress of data based upon protocol, port, source and destination within the environment. Any traffic not adhering to these strict access controls is discarded at the Internet boundary. Internally host-based intrusion prevention and monitoring systems are deployed at the server and network layers, respectively.

System hardening and monitoring

Conga employs standardized system hardening practices across Conga-managed devices. This includes restricting protocol access, removing or disabling unnecessary software and services, removing unnecessary user accounts, patch management, and logging. Additionally, Conga employs an enterprise-class vulnerability management program to monitor and alert on any non-authorized changes or security configurations.

Services undergo 3rd party penetration tests on an annual basis or prior to release of a material change.

Account provisioning and access control

Identity management is used to provide authentication. Users must have a valid username and password to access the system. User profiles containing first and last name, email address, login name, and password are associated with Contract Groups, User Security Roles and Profile Rules using Conditions and actions. Single Sign-On is also an option for ease of user administration and greater security controls. The Conga Contracts Service utilizes SAML 2.0 for our SSO solution.

Conga employee access to the service is limited to only that access required for support and maintenance purposes. Employee access is contingent on a successful background check, confidentiality agreements, and documented authorization by an engineering VP or above. Access is strictly controlled via VPN and other authentication mechanisms.

Data management and protection

The customers of Conga Conga Contracts own the files and data that reside in the service. Each client has their own unique, credentialed and named database instance. These database instances are encrypted at rest for an additional level of data security. Client data is never commingled with other client data.

Incident response

Conga has a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Key staff are trained in forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools. To help ensure the swift resolution of security incidents, the Conga security team is available 24/7 to all employees. If an incident involves customer data, Conga will inform the customer and support investigative efforts via our security team.

Physical security

Processing occurs within AWS data centers that are housed in nondescript facilities. Professional security staff strictly control physical access, both at the perimeter and at building ingress points. Video surveillance intrusion detection systems are in place at a minimum of all ingress and egress points. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification, are signed in, and are continually escorted by authorized staff.

Scalability

The Conga Contracts service is architected to be both horizontally and vertically scalable; additional services can be added to increase the performance of clusters and new clusters can be added to provide service for new clients.

Availability and disaster recovery

Conga maintains geographically diverse data centers and leverages the near seamless failover technologies from AWS. The people, processes, and technology necessary to conduct our business are distributed among these sites, with critical business operations conducted at multiple globally diverse locations. If activity at any one of these sites is disrupted, our systems are designed to continue operating at the other locations without serious interruption for customers.

Available data centers are built in clusters in various regions. All data centers are online and serving customers. No data center is "cold." In the case of failure, automated processes move customer data traffic away from the affected area. Each availability zone is designed as an independent failure zone.

Information stored in the Conga Contracts database systems are backed up using AWS-provided facilities. For short term recoverability, the AWS point-in-time restore capability is enabled. Using a combination of daily snapshots and transaction log backups, a recovery can be performed to any instant in the prior 7 days. For longer term recoverability, AWS snapshots are taken nightly.

For files stored outside of the database, the Amazon EBS snapshot functionality will be used to snapshot the file storage daily. Both the database and file backups will be encrypted and retained for one year

Office disruptions

Conga maintains a globally diverse operations staff in the event core offices have any significant disruption. Additionally, all Conga employees have laptops and a secure process to access necessary resources to support infrastructure and customers.

Conga audits and certifications

Conga is committed to achieving and maintaining the trust and confidence of our customers. Integral to this mission is Conga's dedicated, in-house security and privacy team. This team is tasked with enabling Conga customers to meet a multitude of compliance, data protection, and regulatory obligations from around the globe. Conga's trust and assurance activities include:

- Service Organization Control (SOC) reports: Conga's information security control environment undergoes an independent evaluation annually. Conga's most recent SOC 2, Type II report covering security, availability, and confidentiality is available upon request.
- The Conga Contracts service data centers are SOC 2 Type II audited facilities in the US and ISO 27001 certified in the EU.
- Conga certifies to the U.S. Department of Commerce that it adheres to the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks. Conga's current certification is available at privacyshield.gov/list.
- Data Processing Addendums or Agreements including the Standard Contractual Clauses as approved by the European Commission and incorporating stringent requirements of Article 28 of the EU General Data Protection Regulation 2016/679.
- Cloud Security Alliance's Consensus Assessments Initiative Questionnaire (CAIQ) cloudsecurityalliance.org/registry/conga/
- Penetration testing conducted by industry-recognized 3rd party on material environment changes or annually.
- Conga is ISO 27001 and ISO 27701 certified.
- HIPAA: Conga signs Business Associate Agreements (BAAs) for Contracts.

Security related maintenance

The Conga Contracts service performs security-related change management and maintenance. In most cases, these are transparent to the client via new system builds at the data centers. Patches and updates are installed during the scheduled maintenance window.

For More Information

Email info@conga.com or call
your local Conga office to talk
to a Conga advisor.

Corporate Headquarters

13699 Via Varra
Broomfield, CO 80020
+1 303.465.1616
conga.com

Global Offices

APAC: +61 2 8417 2399
EMEA: +44 (0) 203 608 0165