DATA SHEET

Conga Security Data Sheet

Enterprise grade

As a foundational set of principles, we created our common building blocks on top of the most trusted services in AWS so that availability and security is baked into the core of Conga Cloud. Additionally, we have invested in foundational components such as Conga Drive and Approvals (to name a few) that give us process integrity across workflows and documents. Our runtime systems for transactional and catalog data (and all other) are encrypted in transit and at rest across our SOC 2 compliant cloud.

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, the Conga security team will investigate the incident and work alongside the Conga customer success team to inform the customer.

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.

Encryption for external connections

Customers access the Conga service through the Internet, but only after the authorized end user is properly authenticated. Conga service access requires TLS encryption technology. Connections are encrypted via TLS v1.2 or higher. The private key used to generate the cipher key is at least 2048 bits.

It is recommended that the latest available browsers be utilized for connecting to the Conga service 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 only have least privileged access to the systems. Remote access to the environment is restricted to select operations staff and only available via two-factor authentication.

Anti-virus and anti-malware controls

Conga leverages best in class tools in order to detect 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 detection and monitoring systems are deployed at the server and network layers, respectively.

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.

Data management and protection

All Conga systems used in the provision of the Conga services, including AWS infrastructure components and operating systems, log information to their respective system log facility or a centralized Syslog server (for network systems) to enable security reviews and analysis. The log information is also

aggregated into a Security Information and Event Management (SIEM) solution and analyzed by the Conga security team, which includes additional support from a virtual Security Operations Center (vSOC). Conga services do not maintain customer data postprocessing except for templates. All templates will be disposed of upon termination of services or at customer's request. Data will be disposed of in a manner designed to ensure that they cannot reasonably be accessed or read. The only exceptions to the aforementioned are: 1) if there is a legal obligation imposed on Conga which prevents it from deleting all or part of the environments or data, or 2) if the customer chooses to enable Composer Advanced Features, the use of which stores Composer generated documents in a cloud-based file repository, so they are accessible via a URL. The information customers provide during their use of Conga services that pertains to other individuals and entities is not collected or used by Conga, and remains under the ownership of Conga's customers. Conga processes customer data under the direction of its customers and has no direct control or ownership of the personal data it processes. Customers are responsible for complying with any regulations or laws that require providing notice, disclosure, and/or obtaining consent prior to transferring the data to Conga for processing purposes

Scalability

Conga services are designed to leverage the benefits of a cloud architecture. This includes the capability to scale compute, memory, and network resources to meet the demands of our customers. Conga uses AWS Auto Scaling to maintain application availability and scale our capacity up or down automatically, according to demand. With Auto Scaling, Conga can increase the number of processing.

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:

- 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
- 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.
- Penetration testing conducted by industry-recognized 3rd party on material environment changes or annually. Conga only utilizes infrastructure partners demonstrating the ability to meet rigorous standards (ISO 27001, HIPAA, SOC 2). Conga is ISO 27001 certified.
- HIPAA: Conga signs Business Associate Agreements (BAAs).