Security Policy

Date last modified: 30/06/2018

We take data security and privacy very seriously. As you place your trust in us we recognize that Communic8's information security practices are important to you. For security reasons, we don't expose too much detail around our practices here, but we have provided some general information below to give you confidence in how we secure the data you entrust to us.

Confidentiality & Personnel Practices

We train our employees to understand, recognize and act in your best interest to safeguard your privacy and further protect your data. For example, our employees are trained to recognize and appropriately respond to customer data privacy requests. Furthermore, we train our employees on best security practices, for example, how to identify a data breach and what their responsibilities are if they suspect such an incident occurred.

Furthermore, all employees are required to sign an Employee Security & Confidentiality Undertaking in support of safeguarding your privacy and data.

Physical Security

As a Communic8 customer, you will benefit from a data center and network architecture built to meet the requirements of the most security-sensitive organizations.

To ensure that your data remains secure, we utilise Amazon Web Services (AWS) for our infrastructure needs. AWS is an industry leader in cloud hosting solutions and provides a highly scalable and redundant computing platform with end-to-end security.

Physical access to the AWS data centers is strictly controlled and monitored using sophisticated physical controls, intrusion detection systems, environmental security measures, 24x7 on-site security staff, biometric scanning, multi-factor authentication, video surveillance and other electronic means. All physical and electronic access to the AWS data centers by Amazon employees is authorized on a strictly least privileged basis and is logged and audited routinely.

Some examples of AWS compliance reports and certifications:

- Global: CSA, ISO 9001, 27001, 27017, 27018, PCI DSS Level 1, SOC 1, SOC 2, SOC 3
- United States: CJIS, DoD SRG, FedRAMP, FERPA, FFIEC, FIPS, FISMA, GxP, HIPAA, ITAR, MPAA, NIST, SEC Rule 17a-4(f), VPAT / Section 508
- Asia Pacific: FISC, IRAP, K-ISMS, MTCS Tier 3, My Number Act

- EU: C5, Cyber Essentials Plus, ENS High, G-Cloud, IT-Grundschutz, TISAX

For a full list of Amazon AWS compliance programs and certifications visit: https://aws.amazon.com/compliance/programs/

At Communic8, our employees do not have physical access to our infrastructure in AWS. Electronic access to AWS servers is restricted to a core set of approved staff only.

Data security & encryption (in transit and at rest)

Different client data is stored in separate databases to prevent corruption and overlap. We have multiple layers of logic that segregate user accounts from each other; all client connections to the database are encapsulated, meaning clients cannot access other client data. Our database servers are built on our internal network which cannot be accessed directly from the external internet.

Communic8 supports the latest recommended secure cipher suites and protocols to encrypt all traffic in transit. This means that all communications between your (or your customer's) computer and our service is encrypted using the same technology that banks and financial institutions use. While we implement best practices as new cryptographic features or weaknesses evolve, we are also careful to do this while balancing the need for compatibility for older clients.

All of your data is encrypted at rest (when stored on our servers) using the latest encryption technology and key management best practices. All client data files are located on encrypted disk volumes maintained in the highly secure data centers of AWS.

You can be confident knowing that your data is secure and managed with a best practice approach to storage, backup and retrieval.

Network protection

All servers and databases are firewalled to permit the minimum traffic necessary to run our services. All application APIs are protected by firewall, and all unnecessary ports are blocked by configuration.

Security features of the product

In addition to our security work around data encryption, network protection and physical security in our infrastructure, our product features provide additional security safeguards such as:

- Hashed passwords
- All login pages incorporate brute force protection
- Permission controlled features which authorize access at various levels of the application
- Global and permission-based roles
- UI and backend permission checks
- Account and campaign monitoring for signs of abuse

Disaster recovery

All client database servers support real-time data backup with full daily backups. Backup files are encrypted and securely stored with Server-Side Encryption:

- Nightly production system database backups occur for the last 30 days
- Recovery time for total loss, which includes both server rebuild and data, is 3 hours
- Recovery time for full data loss is just 30 minutes
- All backups are encrypted and inaccessible from outside the network
- Recovery processes are documented, and procedures have been tested

Incident management & response

In the event of a security breach, Communic8 will promptly notify you of any unauthorized access to your customer data. Communic8 has incident management policies and procedures to handle such an event if it were to occur.

External security audits

We contract with respected external penetration testing security firms who perform audits of the Communic8 services to verify that our security practices are sound. They are certified professionals with extensive experience and training, so they can thoroughly test our services for new vulnerabilities discovered by the security research community.

We continually validate the effectiveness of our security program to understand the risks posed to our environment and ensure that the critical systems and data under our control does not suffer a major security breach.

System availability

We're committed to making Communic8 a highly-available service that you can count on. Our infrastructure was engineered and tested from the ground up to be secure, fault tolerant and robust. To show you how confident we are that we can keep the lights on, we provide a generous service level agreement that backs up our claims.

Privacy policy

Your privacy is of critical importance to us. Our Privacy Policy outlines specific details about how we safeguard your information and what you can do if you have concerns or privacy related questions or requests.