ConectUS WIRELESS COMMUNICATIONS®

WE WORK 24/7 TO ENSURE YOUR DATA IS SAFE.

TeamSupport Security

At TeamSupport, we work very hard to ensure your data is safe, and the people we hire and contract with must also ensure their activities are safe, with continual consideration to data integrity and security.

TeamSupport will maintain strict policies and procedures designed to deliver top-notch customer service software security features and to protect the privacy of our client's information. We employ SSL/TLS encryption (AES 256) and other privacy protection technology to secure all of our data. Additionally, these policies and procedures are reviewed annually, or as needed to maintain a healthy service to our customers.

We are able to review and sign Business Associate Agreements, or BAAs, with users of our Enterprise customers who are on annual billing. If you need a BAA in order to comply with the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH), please email sales@teamsupport.com and include the name of the organization or individual to whom the BAA should be addressed.

Application Security

To help ensure the security and privacy of our client's information, we devote significant resources to continually develop our infrastructure. Our customers access TeamSupport only with a valid username and password combination, which is encrypted via SSL/TLS while in transmission.

TeamSupport enforces tight operating system-level security by password protecting all operating system accounts and production databases. We also enforce operating system-level security by using a minimal number of access points to all production servers.

For our customers, each TeamSupport account includes two-factor authentication, password management options, user lock-out and session expiration to ensure they have the tools to help maintain account security within their environment

https://www.teamsupport.com/customer-service-software-security

https://www.teamsupport.com/privacy

Encryption at Rest is also provided to our customers.

Data Center and Network Security

Our world-class data center is built for the cloud and designed to meet the most stringent security requirements in the world, with infrastructure monitoring 24/7 to help ensure the confidentiality, integrity, and availability of your data

In addition, our data center is certified as ISO 27001, PCI/DSS Service Provider Level 1, and/or SOC II compliance.

Infrastructure services include back-up power, HVAC systems, and fire suppression equipment to help protect servers and ultimately your data.

In addition to our extensive internal scanning and testing programs, TeamSupport employs third-party security experts to perform a broad penetration test across the platform.

In case of an alert, we have systems in place to escalate to our 24/7 teams providing operations, network and security coverage. Our employees are trained on security incident response processes.

All customer data is backed up to a geographically separate datacenter on a continual basis. These backups are verified and encrypted.

TeamSupport maintains a robust Disaster Recovery plan for the platform, and encompasses principles of high-availability engineering. The Disaster Recovery plan is routinely measured and is a vital part of the acceptance plan when making changes or additions to the production environment.