# Security is critical to how Plectica works

We take every measure to respect your privacy and secure your information.

## Network Security & Encryption

Network interactions with our site and services happen over a connection using SSL/TLS and RSA encryption. For page requests that means we use HTTPS, and for realtime communication we use secure websockets (WSS).

**We score an "A" rating by Qualsys.**

Following best practices, our internal services are in their own VPC (virtual private cloud), so backend resources are only accessible by our own application servers.

## Authentication & Passwords

We support logging in either with Google via OAuth, or by creating an account directly with Plectica using a password. For direct Plectica accounts, we store hashed passwords using industry standard bcrypt hashing.

## Our Infrastructure

Our services are hosted on the AWS platform which follows industry standard best practices.

We log every access to our system and constantly monitor for any suspicious changes or anomalies.

## Data Storage

Our databases are replicated across data centers so that if one location goes offline, we have spare instances standing by to take over.

As an additional security and redundancy measure, we also take static snapshots of each map within minutes of any change.

We keep daily backups and test restoring from snapshots on a regular basis.

## Availability & Uptime

We take our availability goal seriously: to remain in full functioning order at a rate of 99.95% of the time

To check our availability history and current status, see our status page at plectica.statuspage.io.

## Dedicated Infrastructure for Your Organization

For an extra level of security, our Enterprise customers receive dedicated hardware and network infrastructure so that their data is never on any shared computing, disk, or networking resources.

We work with Enterprise customers to customize VPN configuration and network rules so that Plectica can be easily integrated into the organizations existing IT infrastructure.

## Your Payment Details Are Safe

We don't store any credit card data ourselves – we rely on our partner Stripe to do the heavy lifting there, doing what they do best. See Stripe's security overview for more.

## Internal Testing & Security Bounty

We audit our systems on a recurring basis for any security vulnerabilities, and have an internal bounty incentivizing our team to find and fix any technical issues related to security.

We use OWASP recommendations as strong guidance for where to direct our investigative efforts.