



# Security Overview

If you have any specific questions, please contact us at [security@getclockwise.com](mailto:security@getclockwise.com)

## Data Hosting

Amazon Web Services (AWS)	Clockwise's infrastructure is hosted in Amazon Web Services (AWS) data centers and utilizes the <a href="#">Shared Responsibility Model</a> from AWS.
Encryption	Clockwise keeps your data safe by utilizing encryption protocols like AES 256 and TLS 1.2.

## Security & Compliance Programs

### People

Background Checks	Prior to their start date, all employees must undergo background checks where permitted by law.
Training	All employees are trained on security and data handling to ensure that they uphold our strict commitment to the privacy and security of your data. Employees are made aware of their responsibilities as well as repercussions for failure to adhere to said responsibilities.
Policy Acknowledgements	All Clockwise employees agree to and sign policies covering Confidentiality, Non-Disclosure, Anti-Harassment and Code of Conduct.

### Reliability & Redundancy

Business Continuity & Disaster Recovery	Clockwise has redundant data center regions in place with failover capabilities to ensure the availability of services and
---	--

	data.
--	-------

## Software Development Lifecycle

Feature Releases	Clockwise uses a software development lifecycle (SDLC) in line with general Agile principles. We perform continuous integration which enables us to respond rapidly to functional and security issues. We test our code prior to release, including manual and automated checks.
Quality Assurance (QA) Testing	Clockwise's quality assurance testing ensures every aspect our platform adheres to our quality standards and requirements before a release.

## Vulnerability Management

Vulnerability Scanning	Clockwise checks for vulnerabilities across a range of vectors. Prior to production deployment, code is scanned for any errors and vulnerabilities. Clockwise runs frequent scans on the application level, across endpoints, and across the network.
External Security Assessments	We work with independent third-parties who regularly assess our product for vulnerabilities. Additionally, our bug bounty program rewards security researchers for reporting certain types of vulnerabilities and exploitation techniques.

## Application Security Measures

### Authentication & Authorization

Login Credential Protection	Clockwise will never save your password. Clockwise utilizes Google's OAuth 2.0 endpoints to keep your credentials safe. OAuth 2.0 is a secure authentication and authorization standard which <b>does not</b> expose your password data.
User Provisioning & Deprovisioning	Clockwise offers seamless OAuth through Google Calendar. If a Google account is canceled or suspended, Clockwise immediately loses access. For larger organizations,

	<p>Clockwise supports automatic provisioning and deprovisioning via SCIM if using one of our supported identity providers: Okta, OneLogin, and <a href="#">many more</a>.</p>
--	---