Information Security Overview

Cheqroom - Oct 2024

Confidential

Purpose

Application and Data Security Briefing

This document provides a high-level overview of the primary approaches and measures Cheqroom employs to safeguard member data. It is not intended to serve as a full account of all security procedures and protocols in place.

Security

Monitoring and Alerting

To detect, monitor, alert, and respond to Information Security Incidents, Cheqroom utilizes several key automated security tools, including but not limited to:

1. **AWS Security Hub**: Centralizes security alerts and compliance findings across AWS accounts.
2. **AWS Config**: Monitors AWS resource configurations for compliance with security policies.
3. **AWS Inspector**: Identifies vulnerabilities in AWS applications and infrastructure.
4. **AWS GuardDuty**: Detects and alerts on malicious activity and unauthorized behavior in AWS environments.
5. **Secureframe**: Automates compliance monitoring to maintain security standards across frameworks.
6. **Kandji**: Manages and secures company devices, enforcing security policies and compliance.
7. **Dependabot**: Automatically identifies and updates dependencies to address security vulnerabilities in codebases.
8. **CodeQL**: Performs code analysis to detect vulnerabilities in source code, enhancing code security through continuous scanning.

Transmission of Data

All data is encrypted in transit and at rest

Cheqroom **ensures the secure transmission of data** to and from our network using advanced security technologies. Web traffic is protected by **SSL/TLS encryption**, while data is encrypted both in transit and at rest in our database. We employ state-of-the-art equipment and technology to maintain the confidentiality of your data, which is automatically encrypted as it travels between your device and our servers. Cheqroom uses a robust **SSL cipher key size of 2048 bits**, the largest commercially available, to maximize security.

Data Storage and Security

Zero trust network access environment

All customer data is securely stored in a certified U.S.-based data center, co-managed by Cheqroom and our hosting provider. This facility adheres to a robust compliance program, including HIPAA attestation, FISMA moderate attestation, ISO/IEC 27001:2013 certification, HITECH Act compliance, PCI DSS 3.2 validation, EU-U.S. Privacy Shield Framework, and SSAE 18 SOC 1, SOC 2, and SOC 3 Type 2 examinations. Access to the data center is strictly role-based and granted only as needed for business purposes.

At the database level, application data is **partitioned by unique customer identifiers**, ensuring that customer data can only be accessed by authorized users assigned to the respective customer ID. **Cheqroom takes extensive measures to ensure data security, confidentiality, and disaster recovery capabilities**. Additionally, we operate within a zero trust network access environment, which rigorously controls, monitors, and reports access to our internal systems. Cheqroom attests to SOC 2 Type I and is on track to complete SOC 2 Type II by May 2025.

Data Backup and Recovery

Disaster recovery plan is tested annually.

24/7/365 monitoring of uptime across the infrastructure

At Cheqroom, all production database servers undergo regular backups, full backups daily. Production application build code is backed up nightly to ensure data integrity. We maintain a Recovery Time Objective (RTO) of 12 hours and a Recovery Point Objective (RPO) of 24 hours to minimize data loss and swiftly restore services in the event of an incident. Disaster recovery plan is tested annually.

- **Daily backups** of customer data.
- Recovery Time Objective: **12 hours**
- Recovery Point Objective: **24 hours**

Application Security

Automated code scanning

Cheqroom enforces **industry-standard password controls** for authentication and is secured through **always-on HTTPS**. We emphasize secure development practices through regular developer training and by embedding security champions within development teams. **Our developers adhere to industry best practices, including the OWASP Proactive Controls, to proactively prevent and address application vulnerabilities**.

Cheqroom follows a **Secure Software Development Life Cycle (SDLC),** incorporating best practices for design and solution development based on the **OWASP framework**. To ensure code security, we utilize automated **code scanning by a third-party service**, and all code **undergoes peer review before advancing to QA**, helping us identify and mitigate potential vulnerabilities early in the development process.

FERPA Compliance

Automated code scanning

When Cheqroom receives or accesses personally identifiable information from a student education record, we handle these records in compliance with the Family Educational Rights and **Privacy Act (FERPA), 20 U.S.C. § 1232g**, and its implementing regulations, 34 C.F.R. Part 99, as amended.

We also regularly update our technologies and policies to align with any changes to FERPA regulations.

All Cheqroom employees are required to read, acknowledge, and adhere to FERPA requirements to ensure compliance and protect student privacy.

Data Access

Least privilege access

Cheqroom strictly controls access to all systems including those containing customer data through a ticketing system that authorizes requests for access. Every access event is thoroughly audited and documented, capturing details of who accessed, edited, deleted, or viewed records. Access reviews are conducted at least quarterly to verify appropriateness, particularly for systems containing sensitive data. These systems offer comprehensive audit reporting, providing detailed logs of all user actions to ensure accountability and transparency in data handling.

Access to customer data is governed by a least-privilege approach, allowing us to support customers effectively while safeguarding their data.

Policies Overview

We can share our policies at your request:

- Vulnerability and Patch Management Policy
- Vendor Management Policy
- Security Incident Response Plan
- Secure Development Policy
- Risk Assessment and Treatment Policy
- Privacy and Data Protection Policy
- Physical Security Policy
- Performance Review Policy
- Password Policy
- Network Security Policy
- Internal Control Policy
- Information Security Policy
- Encryption and Key Management Policy
- Data Retention and Deletion Policy
- Data Classification Policy
- Code of Conduct
- Change Management Policy
- Configuration and Asset Management Policy
- Software Development Lifecycle
- Cheqroom Diagrams
- Business Continuity and Disaster Recovery Plan
- Access Control and Termination Policy