PiiQ IT and Security Protocols

Protecting our clients' data through world-class security

Keeping your data safe and secure at all times is our top priority. That's why PiiQ by Cornerstone has security built in as well as real people overseeing PiiQ 24/7. We take care of product security so you can rest easy and focus your time towards continually increasing employee productivity and driving engagement through effective usage of PiiQ.

Here's how we keep your data secure:

Hosting & Availability

PiiQ is hosted using **Amazon Web Services (AWS)** and all clients access the same web-based application in Amazon's "US West 2" region, located in Oregon. We make extensive use of AWS features and functionality including database and file storage, notifications, caching, and DNS. This means PiiQ benefits from Amazon's extensive investment in securing these services. To maintain a very strict separation of client data, each PiiQ client has a separate database, which is automatically created and maintained.

To ensure individual server failures do not disturb the availability of PiiQ, we operate multiple load balanced servers. Application servers and database servers are spread across three separate geographic locations ("availability zones" in AWS terminology), with automatic failover to ensure an outage in one specific location does not affect application availability.

The current status of all AWS services can be monitored here: **https://status.aws.amazon.com**

Encryption & System Authentication

Client databases are encrypted at rest, with AES-256, using the database encryption services, supplied by AWS. Uploaded content is stored in encrypted Amazon Simple Storage Service (S3) buckets. Data in transit is encrypted using TLS, and our servers enforce HTTP Strict Transport Security (HSTS) to prevent unencrypted access.

All client access to PiiQ requires authentication with strong passwords, requiring a minimum of 8 characters with 1 or more uppercase letters, 1 or more lowercase letters, at least one number, and at least 1 symbol. If a user is inactive for one hour, the session will time out and require them to re-enter login credentials. Since PiiQ is entirely web-based i.e. there is no app downloaded from the app store, client data is NOT stored on users' devices.

PiiQ uses a cookie to maintain each authenticated session, and this cookie stores the email address of the user who logged into PiiQ, along with user and client IDs and a randomly generated session token. The contents of the session cookie are encrypted and cleared when logging out. In addition, PiiQ generates a separate cookie, which only stores a randomly generated value to protect against cross-site request forgery (XSRF) attacks.

Backup & Disaster Recovery

Client databases are backed up independently, therefore they can be independently restored. Backups are replicated to a separate AWS region ("US East 1" in North Virginia) for additional redundancy.

- Nightly backups are retained for one week
- Weekly backups are retained for one month
- Monthly backups are retained for six months

We also snapshot all database storage, which allows us to restore all client data in a disaster recovery scenario. In the event of a total loss of all data centers in the "US West 2" AWS region, some manual steps are required to restore the environment.

Monitoring & Alerting

All activity in PiiQ is logged to a persistent storage system. These log records include the IP addresses and email addresses of users accessing the system. This means that every activity performed in PiiQ from the beginning of time has been permanently recorded, and can be internally reviewed/ audited. We also use third party tools to monitor the availability and performance of PiiQ. Availability is tracked from four separate geographic regions and an outage from any one of these regions will trigger automated alerts to on-call staff in the engineering and operations teams. Performance is tracked for every request and monitored by the engineering team. Any severe degradation in performance also results in automated alerts.

Governance

PiiQ's engineering team follows secure coding practices, including manual code reviews and security training for all PiiQ team members. Automated security scans are performed each night and external security reviews and penetration tests are performed twice a year by an independent third party vendor. The engineering team prioritizes any significant security findings, such as potential security vulnerabilities, no matter what.

Release deployments are fully automated to ensure rapid delivery of new features and bug fixes and to minimize the risk of human error. Critical code changes can be deployed in less than one hour! To support the continuous deployment model, we have an extensive suite of automated tests that verify all core product functionality across each phase of deployment.

Internal access to PiiQ is restricted to a small number of staff, required to effectively maintain PiiQ. This includes a subset of employees across the engineering, operations, and support teams. To maintain support across all time zones, designated staff are located in the United States, New Zealand, Israel, India, and the United Kingdom. All internal access to PiiQ is logged and access to the AWS root account requires multi-factor authentication using hardware tokens stored in secure locations. New requests for PiiQ system access follow a formal approval process.

If you would like any further information about product security, or become aware of a potential security vulnerability, please contact us at: **piiqsecurity@csod.com**.