cocoriko

Cyber Security Overview

Data Security

Data Protection in Transit and at Rest

- All application communications are encrypted using TLS 1.3.
- Unsecured HTTP traffic is not allowed.
- HSTS is enabled.
- Databases are hosted on AWS RDS (Canada Central) and are not publicly accessible.
- Data is encrypted at rest (RDS encryption enabled).
- Encryption keys are managed by AWS.
- Production and Staging/Demo environments are separated.
- Access to production environments is restricted and protected by VPN.
- RDS backups (snapshots) are automated and retained for 7 days.

Access Control

- Authentication by unique identifier (email).
- SSO support for administrators and participants.
- Authentication by one-time password (OTP) or social providers.
- Role management:
    - Administrators (organization level)
    - Editors (project level)
    - Participants
- AWS access managed via IAM.
- Production access restricted to the CTO and Dev Lead.
- Logging of access and administrative activities.
- Audit log retention: 12 months.

Data Ownership

- Data remains the exclusive property of the client.
- No secondary use of data.
- Full data export available upon request.
- Data deletion within 30 days following the end of the contract.
- Deletion upon request is possible.
- Certificate of destruction provided upon request.
- Backups follow their automatic retention cycle (7 days).

Conformité et gouvernance

- Hosting exclusively in Canada (AWS Canada Central – ca-central-1).
- Compliance with Law 25 (Quebec).
- Published privacy policy.
- Designated Data Protection Officer.
- Documented Business Continuity Plan (BCP).
- Documented Disaster Recovery Plan (DRP).
    - RTO : 48h
    - RPO : 24h
- Incident log maintained.
- Notification window in the event of an incident: 24h.

Note: Cocoriko is not SOC 2 or ISO 27001 certified to date, but applies AWS and OWASP best practices regarding application and infrastructure security.

Training and Human Resources

- Annual cybersecurity training for employees.
- Confidentiality agreements signed by all employees.
- Formal access revocation procedure upon an employee's departure.
- Encrypted workstations.
- Production access exclusively via secure VPN.

Incident Management and Monitoring

- Documented incident response plan.
- Continuous monitoring via AWS CloudWatch.
- Centralization of application and infrastructure logs.
- Auditing of database administrative actions.
- Backups successfully tested.

Third-Party Vendor Management

Subcontractors Used :

- AWS (infrastructure hosting)
- Postmark (transactional email delivery)
- Umami (analytics)

Measures Applied :

- Access restricted based on the principle of least privilege.
- No subcontractor has direct access to the databases.
- Personal data is not shared with Umami.
- Emails transmitted via Postmark are strictly transactional.

Application Security

- Protection against XSS and CSRF.
- ORM (Sequelize) protecting against SQL injections.
- Mandatory code reviews before deployment.
- Continuous security update management.
- Partial automated testing.
- Dependabot enabled for dependency management.

Resilience

- Database is not publicly accessible.
- Automated backups.
- Segmented architecture by environment.
- Active cybersecurity insurance.