Questionnaire cyber sécurité

Sécurité des données

Protection des données en transit et au repos

- Toutes les communications applicatives sont chiffrées en **TLS 1.3**.
- Le trafic HTTP non sécurisé n'est pas autorisé.
- HSTS est activé.
- Les bases de données sont hébergées sur **AWS RDS (Canada Central)**, non accessibles publiquement.
- Les données sont chiffrées au repos (encryption RDS activée).
- Les clés de chiffrement sont gérées par AWS.
- Les environnements Production et Staging/Démonstration sont séparés.
- Les accès aux environnements de production sont restreints et protégés par VPN.
- Les sauvegardes RDS (snapshots) sont automatisées et conservées 7 jours.

Contrôle d'accès

- Authentification par identifiant unique (courriel).
- Support du SSO pour les administrateurs et participants.
- Authentification par mot de passe à usage unique (OTP) ou fournisseurs sociaux.
- Gestion des rôles :
    - Administrateurs (niveau organisation)
    - Éditeurs (niveau projet)
    - Participants
- Accès AWS gérés via IAM.
- Accès production limités au CTO et au Dev Lead.
- Journalisation des accès et activités administratives.
- Conservation des logs d'audit : 12 mois.

Propriété des données

- Les données demeurent la propriété exclusive du client.
- Aucun usage secondaire des données.
- Export complet des données disponible sur demande.
- Suppression des données dans les 30 jours suivant la fin du contrat.
- Suppression sur demande possible.
- Certificat de destruction fourni sur demande.
- Les sauvegardes suivent leur cycle de rétention automatique (7 jours).

Conformité et gouvernance

- Hébergement exclusivement au Canada (AWS Canada Central – ca-central-1).
- Conformité à la Loi 25 (Québec).
- Politique de protection des renseignements personnels publiée.
- Responsable de la protection des données désigné..
- Plan de continuité des activités (BCP) documenté.
- Plan de reprise après sinistre (DRP) documenté.
    - RTO : 48h
    - RPO : 24h
- Registre des incidents maintenu.
- Délai de notification en cas d'incident : 24h.

Note : Cocoriko n'est pas certifié SOC 2 ou ISO 27001 à ce jour, mais applique les meilleures pratiques AWS et OWASP en matière de sécurité applicative et infrastructure.

Formation et ressources humaines

- Formation annuelle en cybersécurité pour les employés.
- Accords de confidentialité signés par tous les employés.
- Procédure formelle de révocation des accès lors du départ d'un employé.
- Postes de travail chiffrés.
- Accès production uniquement via VPN sécurisé.

Gestion des incidents et surveillance

- Plan de réponse aux incidents documenté.
- Surveillance continue via AWS CloudWatch.
- Centralisation des journaux applicatifs et infrastructure.
- Audit des actions administratives en base de données.
- Sauvegardes testées avec succès.

Gestion des fournisseurs tiers

Sous-traitants utilisés :

- AWS (hébergement infrastructure)
- Postmark (envoi d'emails transactionnels)
- Umami (analytique)

Mesures appliquées :

- Accès limités selon le principe de moindre privilège.
- Aucun sous-traitant n'a accès direct aux bases de données.
- Les données nominatives ne sont pas partagées avec Umami.
- Les emails transmis via Postmark sont strictement transactionnels.

Sécurité applicative

- Protection contre XSS et CSRF.
- ORM (Sequelize) protégeant contre les injections SQL.
- Revues de code obligatoires avant déploiement.
- Gestion des mises à jour de sécurité continue.
- Tests automatisés partiels.
- Dependabot activé pour la gestion des dépendances.

Résilience

- Base de données non accessible publiquement.
- Sauvegardes automatisées.
- Architecture segmentée par environnement.
- Assurance cybersécurité active.