EC09 – Rattrapage : Guide de bonnes pratiques “Sécurité et conformité des données sensibles”

Contexte général

Dans le cadre du projet **FoodSafe**, l’épreuve de rattrapage consiste à rédiger un **guide de bonnes pratiques spécialisé dans la sécurité et la conformité des données**.

Ce document doit formaliser les règles, outils et méthodologies permettant d’assurer la **sécurité applicative**, la **protection des données de santé**, et la **conformité réglementaire (RGPD, HDS)** du projet.
Il s’agit d’un guide opérationnel destiné à être utilisé par les équipes de développement, d’exploitation et de revue de code.

L’objectif est de démontrer la capacité de l’apprenant à articuler **qualité logicielle, sécurité et réglementation** dans un projet à fort enjeu de confiance.

Livrables attendus

Livrable	Détail
Guide de bonnes pratiques	Rédigé en markdown ou PDF, clair, structuré, exploitable par une équipe
Exemples de conventions	Bonnes pratiques de sécurité, Git, gestion des secrets, déploiement
Plan de test / sécurité	Stratégie de vérification et d’audit (tests, scans, outils dédiés)

Modalités d’évaluation

- **Type d'épreuve** : Mise en situation reconstituée écrite
- **Durée** : 4h
- **Nature** : Épreuve individuelle, sans oral
- **Critères évalués** :
  - C8.6 : Conventions de code et documentation
  - C9.6 : Stratégie de tests et de sécurité
  - C14.3 : Qualité logicielle globale (approche mesurable et réaliste)

Recommandations

- Structurer le guide par **thématiques concrètes** : sécurité, conformité, code review, documentation, CI/CD
- Décrire les **mesures techniques obligatoires** : chiffrement, hashage, anonymisation, validation des entrées
- Proposer des **outils de contrôle automatisé** : linters, scanners SAST/DAST, analyse de dépendances, gestion des secrets
- Donner des **exemples de configuration** (Git hooks, pipeline CI, gestion des tokens et variables sensibles)
- Intégrer une **checklist RGPD et accessibilité** pour chaque sprint ou release
- Rester pragmatique : le guide doit être **utilisable et vérifiable** par une équipe réelle

Exemples d'éléments attendus

- Bonnes pratiques de sécurité dans le code : gestion des tokens JWT, stockage des mots de passe, validation serveur
- Convention Git avec règles pour les commits liés à la sécurité (`fix(security): …`)
- Modèle de **checklist de revue de code** intégrant les risques RGPD et sécurité
- Exemple d'intégration d'un outil de scan automatique (Snyk, Trivy, CodeQL, SonarCloud)
- Plan de test automatisé vérifiant la conformité (unitaires + tests de sécurité)

Nom de dossier attendu

- Une archive ZIP nommée `EC09R_NomPrenom.zip` contenant :
  - Le guide au format `.md` ou `.pdf`
  - Un dossier `exemples/` avec extraits de code, configurations ou pipelines CI/CD
  - Un fichier `README.md` expliquant la logique et la structure du guide

Rappel pédagogique

Cette épreuve de rattrapage vise à évaluer les mêmes compétences que l'EC09 initiale, avec un focus renforcé sur :

- La **sécurisation du cycle de développement** et la prévention des vulnérabilités
- L'**intégration des exigences réglementaires** (RGPD, HDS) dans les pratiques de qualité logicielle
- La **formalisation claire et opérationnelle** de procédures applicables en équipe

Le scénario change (guide spécialisé "sécurité & conformité" plutôt que guide global de qualité), mais les objectifs et le niveau d'exigence restent identiques.