Dossier sur l'accessibilité

et la sécurité

I. Accessibilité

1. Interface utilisateur adaptée

- **Design ergonomique et intuitif accessible à tout utilisateur, quel que soit son niveau technique.**
- **Compatibilité avec les lecteurs d'écran (VoiceOver, NVDA) pour utilisateurs non-voyants ou malvoyants.**
- **Respect des normes WCAG 2.1 (Web Content Accessibility Guidelines), notamment avec un contraste des couleurs élevé, texte alternatif systématique sur les images, et navigation par clavier.**

Fonctionnalités d'accessibilité avancées :

- **Modes sombre et clair pour améliorer le confort visuel.**
- **Taille des polices ajustable pour répondre aux différents besoins visuels.**

2. Multilinguisme et internationalisation

- **Interface disponible en plusieurs langues.**
- **Détection automatique de la langue du navigateur.**
- **Adaptation culturelle et régionale des contenus.**

3. Accessibilité technique

- **Fonctionnement fluide sur navigateurs et plateformes diverses (mobile, desktop, tablette).**
- **Optimisation de la vitesse et réduction des temps de chargement pour garantir l'accessibilité en cas de faibles connexions réseau.**

Sécurité

1. Protection des données utilisateur

- **Sécurisation des données personnelles et de paiement par tokenisation.**

2. Authentification et contrôle d'accès

- **Implémentation d'authentification forte à deux facteurs (2FA).**
- **Utilisation de JWT pour la gestion sécurisée des sessions utilisateur.**
- **Gestion stricte des permissions et des rôles avec la possibilité d'authentification multifacteur.**

3. Sécurité applicative et prévention des intrusions

- **Protection contre les attaques par injection (SQLi, XSS, CSRF).**
- **Systèmes anti-DDoS pour assurer la continuité du service.**
- **Firewall applicatif Web (WAF) intégré pour filtrer le trafic malveillant.**

3. Gestion sécurisée des téléchargements

- **Vérification automatique de l'intégrité des fichiers téléchargés.**
- **Utilisation de serveurs sécurisés et authentifiés pour éviter les redirections malveillantes.**
- **Contrôle antivirus sur tous les fichiers uploadés.**

4. Sécurité des API et intégrations tierces

- **Authentification sécurisée par tokens JWT.**
- **Monitoring et contrôle strict des accès aux API.**
- **Politique de gestion stricte des clés API.**

Audits et surveillance continue

- **Audits périodiques de sécurité par des sociétés tierces spécialisées.**
- **Tests réguliers de pénétration et de vulnérabilités (pentests).**
- **Surveillance continue via SIEM et alertes en temps réel.**

Sauvegarde et gestion des incidents

- **Sauvegardes régulières des données avec redondance géographique.**
- **Plan de reprise d’activité (PRA) détaillé en cas d’incident majeur.**
- **Protocoles clairs de réponse aux incidents avec une équipe dédiée à la sécurité.**

Formation et sensibilisation

- **Formation régulière des équipes techniques à la sécurité informatique.**
- **Sensibilisation continue des utilisateurs aux bonnes pratiques de sécurité.**