ANNEXE B

POLITIQUE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION (PSSI)

1. Objet

La présente Politique de Sécurité des Systèmes d'Information (PSSI) décrit les mesures techniques et organisationnelles mises en œuvre par MYESIS SOLUTIONS afin d'assurer un niveau de sécurité adapté aux risques liés à l'exploitation de la plateforme LumivaPDF.

Elle complète les Conditions Générales de Vente et d'Utilisation ainsi que l'Accord de Traitement des Données (DPA) et s'inscrit dans une démarche d'amélioration continue de la sécurité.

Les mesures décrites dans cette annexe sont susceptibles d'évoluer afin de tenir compte des progrès technologiques, des évolutions réglementaires et des nouvelles menaces.

---

2. Principes généraux

La politique de sécurité repose sur quatre objectifs fondamentaux :

- assurer la **confidentialité** des données ;
- garantir leur **intégrité** ;
- maintenir leur **disponibilité** ;
- permettre leur **traçabilité**.

Les dispositifs de sécurité sont conçus selon une approche de défense en profondeur, combinant des mesures organisationnelles, techniques et opérationnelles.

---

3. Gouvernance de la sécurité

MYESIS SOLUTIONS définit et met en œuvre une organisation interne visant à garantir un niveau de sécurité adapté à la nature des services proposés.

Cette gouvernance comprend notamment :

- la définition de responsabilités en matière de sécurité ;

- la revue régulière des risques ;
- la mise à jour des procédures internes ;
- la sensibilisation des collaborateurs ;
- l'amélioration continue des pratiques de sécurité.

---

4. Gestion des accès

L'accès aux systèmes d'information est limité aux seules personnes habilitées.

Les droits d'accès sont attribués selon le principe du **moindre privilège**, chaque utilisateur ne disposant que des autorisations strictement nécessaires à l'exercice de ses missions.

Les mesures suivantes sont notamment mises en œuvre :

- authentification individuelle des utilisateurs ;
- gestion des profils et des habilitations ;
- révocation des accès devenus inutiles ;
- contrôle périodique des comptes actifs ;
- journalisation des connexions d'administration.

Lorsque disponible, une authentification multifacteur (MFA) peut être imposée pour les comptes présentant un niveau de privilège élevé.

---

5. Gestion des mots de passe

Les utilisateurs sont invités à choisir des mots de passe robustes répondant aux bonnes pratiques de sécurité.

Les mots de passe doivent notamment :

- présenter une longueur suffisante ;
- comporter des caractères variés ;
- ne pas être réutilisés sur plusieurs services ;
- rester strictement confidentiels.

Les mots de passe ne sont jamais stockés en clair.

Ils sont conservés sous forme de condensats cryptographiques (« hash ») utilisant des mécanismes reconnus par l'état de l'art.

---

6. Sécurité des communications

Les échanges entre les utilisateurs et la plateforme sont protégés par des protocoles de chiffrement conformes aux standards actuels.

Les communications utilisent notamment le protocole TLS afin de garantir :

- la confidentialité des échanges ;
- l'intégrité des données transmises ;
- l'authenticité du serveur.

Les certificats numériques font l'objet d'un suivi régulier et sont renouvelés avant leur expiration.

---

7. Protection des données

Les données hébergées par LumivaPDF font l'objet de mesures destinées à prévenir :

- la perte ;
- l'altération ;
- l'accès non autorisé ;
- la divulgation accidentelle.

Selon la nature des données et l'architecture technique retenue, des mécanismes de chiffrement au repos peuvent être mis en œuvre.

Les sauvegardes bénéficient d'un niveau de protection équivalent.

---

8. Journalisation et traçabilité

Afin de détecter les anomalies et de faciliter les investigations, différents événements techniques peuvent être enregistrés, notamment :

- les authentifications ;
- les erreurs applicatives ;
- les opérations d'administration ;
- les incidents techniques ;
- les opérations sensibles réalisées sur la plateforme.

Les journaux sont protégés contre toute modification non autorisée et conservés pendant une durée compatible avec les exigences techniques, contractuelles et réglementaires.

9. Gestion des vulnérabilités

MYESIS SOLUTIONS met en œuvre une démarche continue de gestion des vulnérabilités comprenant notamment :

- une veille de sécurité ;
- l'application régulière des correctifs logiciels ;
- la mise à jour des composants techniques ;
- l'analyse des alertes de sécurité ;
- la correction prioritaire des vulnérabilités critiques.

Les délais de correction sont adaptés au niveau de criticité identifié.

---

10. Protection contre les logiciels malveillants

Les infrastructures exploitées par MYESIS SOLUTIONS bénéficient de dispositifs destinés à prévenir les risques liés aux logiciels malveillants.

Ces dispositifs peuvent notamment comprendre :

- des mécanismes de filtrage ;
- des protections antivirus lorsque cela est pertinent ;
- des systèmes de détection d'activités anormales ;
- des procédures d'isolement en cas d'incident.

---

11. Sauvegardes

Des sauvegardes régulières sont réalisées afin d'assurer la continuité des services.

Les procédures de sauvegarde font l'objet :

- d'un contrôle périodique ;
- de tests de restauration ;
- d'une surveillance des opérations automatiques.

Les modalités détaillées sont précisées dans l'Annexe D relative à la sauvegarde et à la réversibilité des données.

---

12. Gestion des incidents de sécurité

Tout incident de sécurité identifié fait l'objet d'une procédure interne visant à :

- qualifier l'incident ;
- limiter son impact ;
- restaurer les services ;
- analyser les causes ;
- mettre en œuvre les actions correctives nécessaires.

Lorsqu'un incident est susceptible d'affecter les données personnelles traitées pour le compte d'un Client, celui-ci est informé dans les meilleurs délais conformément aux dispositions du RGPD et du DPA.

---

13. Continuité d'activité

MYESIS SOLUTIONS met en œuvre des mesures destinées à favoriser la continuité de fonctionnement de la plateforme.

Ces mesures peuvent notamment comprendre :

- des sauvegardes régulières ;
- des procédures documentées de restauration ;
- des mécanismes de supervision ;
- des plans de reprise adaptés à la nature des incidents.

Les objectifs opérationnels de continuité sont définis dans le SLA.

---

14. Sous-traitants techniques

Lorsque MYESIS SOLUTIONS fait appel à des prestataires techniques (hébergement, supervision, messagerie, sécurité ou services cloud), elle veille à sélectionner des partenaires présentant des garanties suffisantes en matière de sécurité et de conformité réglementaire.

Les sous-traitants sont soumis à des obligations contractuelles de confidentialité et de sécurité compatibles avec celles prévues dans les présentes Conditions Générales.

---

15. Sensibilisation

Les collaborateurs susceptibles d'accéder aux systèmes d'information ou aux données des Clients sont sensibilisés aux bonnes pratiques de cybersécurité.

Cette sensibilisation porte notamment sur :

- la protection des identifiants ;
- la détection des tentatives d'hameçonnage ;
- la confidentialité des informations ;
- la gestion des incidents ;
- les obligations découlant du RGPD.

---

16. Amélioration continue

La présente politique fait l'objet de revues régulières.

MYESIS SOLUTIONS se réserve le droit d'adapter ou de renforcer les mesures décrites afin de tenir compte :

- des évolutions technologiques ;
- des recommandations de l'ANSSI ;
- des bonnes pratiques du secteur ;
- des exigences de la norme ISO/IEC 27001 ;
- des évolutions réglementaires.

Toute évolution ayant pour objet de renforcer le niveau de sécurité bénéficie automatiquement aux Clients et ne nécessite pas la conclusion d'un avenant.

---

17. Entrée en vigueur

La présente Politique de Sécurité des Systèmes d'Information entre en vigueur à la même date que les Conditions Générales de Vente et d'Utilisation auxquelles elle est annexée.

Elle constitue un document contractuel et s'impose à l'ensemble des Parties pendant toute la durée de la relation contractuelle.