

P1 : Politique de sécurité des services d'information

1. Contexte

☐ Objectifs

Une politique de sécurité de l'information (PSI) vise à promulguer des protections et à limiter la distribution des données aux personnes autorisées à y accéder. La société, LAYAN SAS, crée cette politique pour :

- Établir une approche générale de la sécurité de l'information
- Documenter les mesures de sécurité et les politiques de contrôle d'accès des utilisateurs
- Détecter et minimiser l'impact des actifs informationnels compromis tels que l'utilisation abusive des données, des réseaux, des appareils mobiles, des ordinateurs et des applications.
- Protéger la réputation de l'organisation
- Se conformer aux exigences légales et réglementaires.
- Protéger les données de leurs clients, telles que les numéros de carte de crédit.
- Fournir des mécanismes efficaces pour répondre aux plaintes et aux demandes liées à des risques réels ou perçus en matière de cybersécurité, tels que le phishing, les logiciels malveillants et les ransomwares.
- Limiter l'accès aux principaux actifs informatiques aux personnes dont l'utilisation est acceptable.

☐ Définitions

« Les collaborateurs » sont définis comme l'ensemble des salariés et contractuels de LAYAN SAS (employés, alternants, directeurs, stagiaires).

« Les prestataires » sont définis comme toute personne morale ou établissement fournissant à LAYAN SAS des biens ou services nécessaires à son activité

« La société » est définie comme LAYAN SAS

« Actifs essentiels » sont définis comme les ressources informationnelles ou processus ayant de la valeur pour la société.

2. Responsabilités et gouvernance

La présente politique s'adresse à :

- ☐ L'ensemble des collaborateurs de LAYAN SAS
- ☐ L'ensemble des fournisseurs et prestataires de LAYAN SAS
- ☐ Les clients de LAYAN SAS

Le Directeur Général de LAYAN SAS, Nicolas CHEVALIER, est le responsable de la bonne application de cette politique et de sa mise à jour régulière selon les évolutions réglementaires ou organisationnelles internes.

Le Lead Développeur de LAYAN SAS, Samuel Simonney a pour responsabilités :

- ☐ La remontée d'information et des incidents à la Direction
- ☐ La gestion des incidents et la résolution ou l'escalade des incidents
- ☐ La sensibilisation des collaborateurs (salariés, contractuels, alternants, stagiaires...) de la société sur une base annuelle sous la forme d'une formation

Tous les employés de LAYAN SAS sont tenus de respecter la présente politique.

3. Contrôles

La protection des systèmes d'information est assurée par 3 niveaux de contrôles :

Niveau de contrôle	Responsabilités	Fréquence	Points de contrôle
Contrôle opérationnel	L'ensemble des collaborateurs de la société	En continu	☐ S'assurer du bon respect de la politique de respect de la confidentialité
Contrôle permanent	Directeur général et Lead Développeur	Une fois par an	☐ Conduite de contrôle et de tests ☐ S'assurer de la formation et la prévention auprès des collaborateurs ☐ Recueillir et protéger les informations des clients et collaborateurs ☐ S'assurer du bon respect des évolutions réglementaires
Contrôle périodique	Audit par une société externe et indépendante	Une fois tous les 2 à 3 ans	S'assurer du bon respect et du bon contrôle de la présente politique ainsi que sa mise en conformité avec la réglementation en vigueur

4. Plan de continuité de l'activité (PCA) et accès à distance

- ☐ Objectifs

Le PCA permet de mettre en place les moyens permettant de faire fonctionner la société en cas de crise et de rupture de l'activité.

Le PCA doit être distribué et à disposition de tous les collaborateurs de la société.

☐ **Déroulé du PCA**

Etape	Déroulé
Identification d'une situation de crise	Le Directeur Général est averti d'une situation à risque et prend la décision de déclencher le PCA
Déclenchement du PCA	- Le Directeur Général est tenu de communiquer à tous les collaborateurs les instructions relatives au déclenchement du PCA - Les prestataires et clients de la société doivent être tenus au courant
Durée du PCA	- Les systèmes d'information sont surveillés et les collaborateurs reçoivent les accès si nécessaires - Mise en place d'une cellule de communication afin de préserver les données et les systèmes d'information - Les collaborateurs vérifient être en conformité avec les règles relatives aux conflits d'intérêts pendant toute la durée du PCA
Rétablissement des activités	- Les collaborateurs sont invités à reprendre leurs activités
Établissement d'un rapport	- Le Directeur Général établit un rapport reprenant les étapes et les archives (mails, échanges téléphoniques) ayant un lien avec le PCA
Contrôle	- Le déroulé du PCA est audité et contrôlé a posteriori

☐ **Responsabilités**

Le Directeur Général est responsable du bon déroulé et du respect du PCA.

Les collaborateurs sont responsables du respect de la présente politique durant toute la durée du PCA.

5. Tests

Le Lead Développeur, sous la responsabilité du Directeur Général conduit :

- ☐ Des tests de pénétration sur une base annuelle ou biannuelle selon la politique de gestion des risques
- ☐ Des tests de vulnérabilité (phishing, cybersécurité, accès)

Ces tests pourront être conduits par des prestataires externes.

Ces tests ont pour objectifs d'identifier et adresser les incidents éventuels et les zones de risques de la société.

Ces tests feront l'objet d'un rapport daté, signé et archivé à des fins de contrôle.

6. Contrôle des accès et des systèmes

□ Contrôle des accès

Les accès aux serveurs de la société sont sécurisés par des mots de passe robustes et des clés ssh inscrits sur 2 PC.

Celui du Lead Developer est sur un ordinateur de sauvegarde protégé par le Directeur Général.

Notre environnement s'exécute sur des containers Docker qui sont envoyées sur des instances AWS.

L'accès à l'interface administrateur de AWS est sécurisé par un mot de passe et une double authentification avec un SMS envoyé uniquement sur le téléphone du Directeur Général.

Chaque action faite sur ces instances doit être testée dans nos environnements de test et être approuvée par la direction.

□ Surveillance des accès

Chacun de nos utilisateurs dispose d'accès précis en fonction du poste qu'il occupe.

Les accès administrateurs, back office et base de données sont restreints uniquement au Lead Developer et au Directeur Général.

La totalité des routes de la société sont sécurisées et requièrent une authentification.

Si un utilisateur demande à accéder à une page/interface dont il n'a pas le droit, il sera redirigé vers une page "401 Unauthorized".

□ Encadrement du développement des systèmes

Lors de chaque développement, les développeurs ont des règles strictes à respecter pour assurer au mieux la robustesse et la prospérité du bon fonctionnement de leur code. C'est pourquoi à chaque nouvelle fonctionnalité, au minimum 2 tests fonctionnels et 2 tests unitaires doivent être mis en place. Chaque nouvelle route ouverte sur notre application doit être sécurisée par une authentification et la société s'assure de vérifier que l'utilisateur connecté possède bien les droits pour effectuer l'action souhaitée.

Concernant certaines pages qui ne demandent pas d'authentification comme la page d'inscription ou connexion, des mesures en plus sont mises en place comme un blocage après plusieurs tentatives effectuées par le même utilisateur.

Toutes les données reçues par la société (formulaires, fichiers) sont vérifiées pour éviter toute injection malveillante.

□ Encadrement du code

Des règles de « coding style » sont mises en place et doivent être respectées pour permettre au mieux la durabilité et la compréhension du code.

Des commentaires doivent être mis en place sur chaque bout de code.

Les règles de bonnes pratiques générales doivent être respectées par tous et sur tout code effectué.

Des outils dans l'intégration continue nous permettent de suivre la qualité du code et de bloquer chaque déploiement si ces exigences ne sont pas respectées.

□ Suivi des erreurs et de la sécurité

À chaque erreur parvenue sur notre logiciel des mails et notifications Slack sont envoyés au personnel concerné pour agir et prendre conscience du problème pour le résoudre au plus vite.

Des outils de surveillance et de remonté de log sont mis en place pour suivre au mieux les activités et anticiper les éventuels désagréments qui pourraient survenir.

En cas d'événement indésirable une procédure d'urgence et un plan de reprise des activités sont prévus (voir PCA).

□ **Données clients**

Aucun test n'est effectué sur des données client.

Tous les tests sont effectués sur des environnement de test avec des données de test.

Des tests fonctionnels et unitaires sont lancés lors de chaque ouverture de "Pull request".

Le code doit être relu par 2 développeurs minimum dont le Lead Développeur.

Ces fonctions sont ensuite validées par une équipe de testeurs sur des environnements locaux puis sur des environnements distants avec des données de tests

Après validation de toutes ces étapes, une mise en production peut être lancée.

7. Gestion des risques et des incidents

Etape	Personne en charge	Responsabilités
Sensibilisation des collaborateurs pour être en mesure de détecter les incidents	Lead Développeur	Conduire des formations et tests sur une base régulière
Détection des incidents	Ensemble des collaborateurs	Faire preuve d'une culture éthique et savoir repérer les incidents
Remontée de l'incident	Ensemble des collaborateurs	Faire remonter l'incident au Lead Développeur
Escalade de l'incident	Lead Développeur	Remontée au Directeur Général si l'incident ne peut pas être résolu en première instance par le Lead Développeur
Rapport d'incident	Lead Développeur	Archive d'un rapport d'incident daté et signé à des fins de contrôle
Contrôles de la gestion des incidents	Instances de contrôle (voir partie 3 « Contrôles »)	Voir partie 3 « Contrôles »

Le Directeur Général est tenu de réaliser une fois par an une étude de gestion des risques pouvant prendre la forme d'une cartographie des risques et permettant d'apprécier la gravité et la probabilité des risques identifiés. Cette étude des risques peut être fournie par un tiers prestataire et fera l'objet d'un contrôle.

8. Sécurité physique

☐ Locaux

Les locaux de la société sont implantés à la suite d'une étude de sécurité du site afin de s'assurer que :

- Le prestataire de location des bureaux dispose de pratiques de sécurité informatique en respect avec la réglementation en vigueur
- Les autres sociétés de l'immeuble ne présentent pas de risque
- Les bureaux disposent d'un contrôle d'accès et que seuls les collaborateurs de la société peuvent pénétrer dans les bureaux

☐ Limites et contrôles

Les mécanismes de contrôles tels que la limitation des accès, les verrous, les détections d'intrusion sont testés régulièrement et font l'objet de rapports détaillés.

☐ Equipements

Les ordinateurs, téléphones et tout équipement mis à disposition des collaborateurs de la société respectent les obligations suivantes :

- Changement des mots de passe à intervalle régulier
- Sécurisation des appareils et protection contre les menaces extérieures
- Accès sécurisés en cas de travail à distance (télétravail) sur un serveur sécurisé
- Les équipements sont rendus à la fin du contrat de travail

9. Ressources humaines

☐ Avant l'embauche

Avant l'embauche, la société s'assure que les salariés et contractuels comprennent leurs responsabilités et sont compétents pour remplir leurs fonctions.

Les salariés travaillant sur des postes sensibles ou amenés à manipuler des données sensibles sont contrôlés via un contrôle de leur identité et des vérifications d'antécédents et d'expériences auprès de références externes.

☐ Pendant la durée du contrat

Les collaborateurs sont tenus de connaître leurs responsabilités en matière de sécurité de l'information. Des exercices de sensibilisation sont conduites par le Lead développeur sur une base annuelle et connaissent les moyens de faire remonter des incidents.

En cas de non-respect des règles de sécurité des systèmes d'information, le collaborateur s'expose à des processus disciplinaires pouvant entraîner des actions immédiates telles que la rupture du contrat de travail.

☐ Fin du contrat de travail

A la fin du contrat de travail, les dirigeants de la société s'assurent de la bonne restitution du matériel informatique et que ses accès soient immédiatement bloqués. Un collaborateur temporaire n'est pas autorisé conserver des données professionnelles après son départ.

10. Hébergement de l'Application

□ Extrait des CGV relatif à l'hébergement des données

Layan s'engage à assurer, dans les termes d'une obligation de moyens, l'hébergement des Comptes et de tout contenu publié par le Recruteur sur son Compte conformément aux usages de la profession et à l'état de l'art, sur ses propres serveurs ou par un prestataire d'hébergement professionnel, exerçant son activité conformément aux usages de la profession et à l'état de l'art.

Dans ce cadre, Layan s'engage à fournir au Recruteur des capacités de stockage et de traitement suffisantes dans le cadre des Services, conformément aux usages de la profession et à l'état de l'art.

Layan s'engage à mettre en œuvre l'ensemble des moyens techniques, conformes à l'état de l'art, nécessaires pour assurer la sécurité et l'accès aux Services, portant sur la protection et la surveillance des infrastructures, le contrôle de l'accès physique et/ou immatériel auxdites infrastructures, ainsi que sur la mise en œuvre des mesures de détection, de prévention et de récupération pour protéger les serveurs d'actes malveillants.

Layan s'engage également à prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par les traitements automatisés de données mis en œuvre pour les besoins des Services, pour préserver la sécurité des données, et notamment empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès.

□ AWS Services

Layan assure l'hébergement des données des Comptes sur le service Cloud de Amazon Web Services, ce prestataire d'hébergement professionnel exerce son activité conformément aux usages de la profession et à l'état de l'art.

Layan a choisi délibérément d'héberger la totalité des données sur des serveurs EC2 situés en France et plus précisément en région parisienne. Ci-après les codes Zones d'hébergement de l'ensemble des serveurs utilisés par Layan :

Region

Europe (Paris)

Zones

Zone name	Zone ID
eu-west-3a	euw3-az1
eu-west-3b	euw3-az2
eu-west-3c	euw3-az3

Cette procédure a été revue est validée par la Direction en octobre 2023.