POLITIQUE GLOBALE DE SECURITE DE L'INFORMATION DU GROUPE **XXXX** [PGSI]

TABLE DES MATIERES

HISTORIQUE DES REVISIONS

Version	Date	Auteurs	Date de validation	Validé par
1.0	Mai 2022			

➔ Documents de référence

Intitulé
CHARTE DE BON USAGE DES RESSOURCES INFORMATIQUES
CHARTE DE SECURITE INFORMATIQUE
CHARTE DEDIEE AUX ADMINISTRATEURS (TECHNIQUES ET FONCTIONNELS)
CHARTE DU DEVELOPPEUR
CHARTE UTILISATEUR
INTEGRATION DE LA SECURITE DANS LES PROJETS SI
LETTRE D'ENGAGEMENT
METHODE D'ANALYSE DE RISQUES
PLAN D'ASSURANCE SECURITE
PLAN DE SECOURS INFOMATIQUE
PLAN REPRISE D'ACTIVITE
POLITIQUE DE GESTION DES MOTS DE PASSE
POLITIQUE DE TELETRAVAIL
PROCEDURE DE CLASSIFICATION
REFERENTIELS DE LA SECURITE DANS LES DEVELOPPEMENTS
REGLEMENT INTERIEUR
REGLES D'USAGES DES TELEPHONES MOBILES

I. INTRODUCTION A LA PGSI

1.1. LES PRINCIPES FONDATEURS DE LA PGSI

La Politique Globale de Sécurité de l'Information (PGSI) fixe le cadre de référence du groupe XXX pour la protection de l'Information et la sécurité de ses systèmes d'information.

Fondée il y a XXX ans, le groupe XXX est devenue Numéro 1 de la franchise sur le marché de XXX. Cette situation lui confère un positionnement national qui la pousse à garantir un management de la sécurité adapté vis-à-vis de ses clients ainsi que de ses franchisés.

La présente PGSI exprime la réelle volonté de la direction générale du groupe XXX de :

- Contribuer à la stratégie et à l'image de marque du groupe,
- Protéger ses données ainsi que celles de ses clients, de ses employés ainsi que de ses franchisés,
- Protéger le patrimoine du groupe,
- Lutter contre les malveillances informatiques,
- Prévenir les risques :
  - D'appropriation illégale de biens financiers, matériels ou informationnels,
  - De dommage ou destruction de biens matériels ou informationnels,
  - D'accès non autorisé aux biens informationnels, de divulgation ou de modification non autorisée.
- S'assurer que les utilisateurs aient connaissance et appliquent les bonnes pratiques et les règles quant à l'usage des systèmes d'information,
- Respecter les obligations légales et réglementaires,
- Assurer la reprise des activités.

1.1.1. LES ELEMENTS STRUCTURANTS DU REFERENTIEL DE SECURITE

Il s'agit des domaines de sécurité constituant le socle de la PGSI. Ces principes regroupent l'ensemble de mesures techniques et organisationnelles précises à mettre en œuvre pour protéger :

- Les données,
- Les services (Continuité des opérations),
- Les équipements (Sécurité des systèmes et postes de travail),
- Les applications (Contrôle des accès logiques),
- Les locaux (Sécurité physique),
- Les personnes.

Les chartes et contrats de sécurité constituent une déclinaison des règles de sécurité établies dans la PGSI et des directives de sécurité, à destination des collaborateurs et des tiers. On y retrouve les chartes de sécurité utilisateur et administrateur, les clauses contractuelles liées à la sécurité, ainsi que les modèles d'engagement de confidentialité. Les processus de sécurité fournissent une description détaillée des différentes activités liées à la sécurité.

1.1.2. LES POLITIQUES TECHNIQUES DE SECURITE (PTS)

La politique de sécurité se décline en documents standards et guides de sécurité appelés PTS, Politique Technique de Sécurité. Chaque domaine technique principal (réseau, poste de travail, serveurs, base de données, applications métiers,) présent dans le groupe XXX devra avoir son PTS reprenant les exigences de sécurité qui doivent être implémentées.

Les Politiques Technique de Sécurité sont la déclinaison de la politique de sécurité par « processus » de sécurité. Ces standards de sécurité détaillent la politique de sécurité en fonction d'un contexte plus spécifique.

Une PTS définit l'applicabilité des règles qui peuvent être des directives, des recommandations ou des bonnes pratiques.

Les directives :

Les directives de sécurité fournissent une description détaillée des règles édictées dans la PGSI. Une directive est impérative et doit être appliquée conformément à son contenu et aux conditions d'application sur l'ensemble des systèmes d'information de XXX. La non-

application d’une Directive doit avoir pour corollaire l’existence d’une dérogation ou d’un plan d’action de contournement.

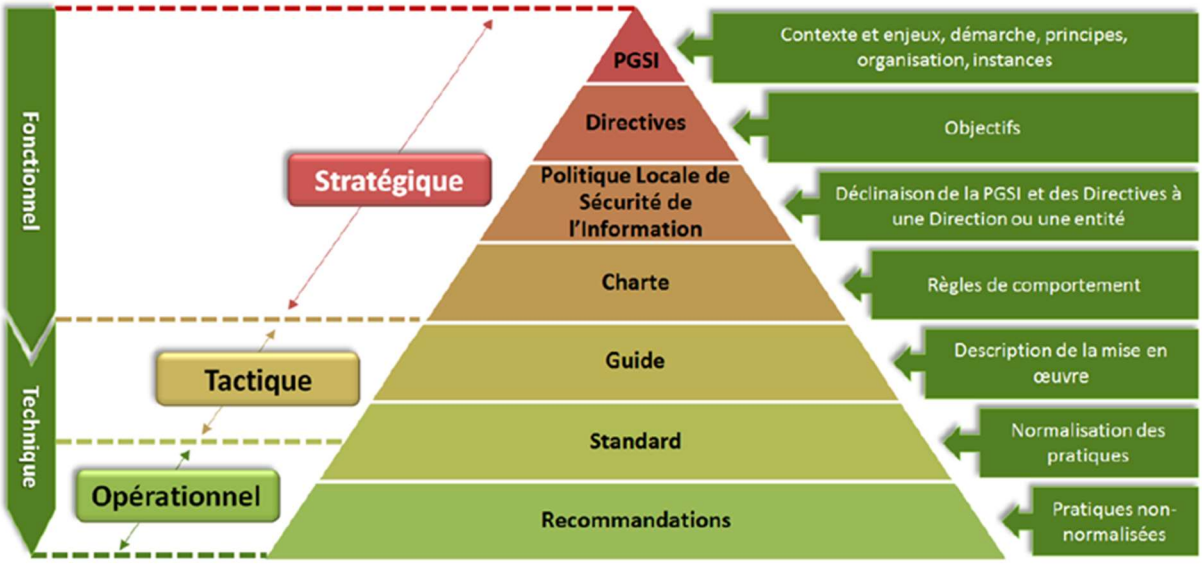
Les recommandations :

Une recommandation s'applique le plus largement possible sur l'ensemble du SI de XXX. Des contraintes spécifiques peuvent nécessiter d'y déroger. Dans ce cas, les conséquences techniques sont pleinement assumées par l'entité responsable de sa non-application.

L'entité sera néanmoins amenée, dans le cadre des contrôles et des audits, à rendre compte de la raison pour laquelle elle n'applique pas une recommandation.

Les bonnes pratiques :

A minima, les règles de bonnes pratiques référencées dans les référentiels et normes de sécurité, dans les documentations constructeurs et éditeurs, dans les forums ou documents d’experts de la sécurité devront être prises en compte, considérées afin d’être déployées dans les projets et surtout appliquées dans les configurations des matériels, et l’élaboration des processus.



1.2. OBJECTIFS DE LA PGSI

Cette politique présente les enjeux, les besoins et les principales obligations légales et réglementaires en matière de sécurité de l'Information, puis définit les principes, les acteurs, les rôles et responsabilités (l'organisation de la sécurité), ainsi que la gouvernance sécurité de l'information (les instances de pilotage) au sein du Groupe.

Les mesures présentées sont génériques, et s'appuient sur des politiques, des chartes et des référentiels de sécurité.

La présente politique est approuvée par la Direction Générale du Groupe XXX.

Parmi les différents objectifs liés à la PGSI que le groupe XXX mets en œuvre on retrouve :

- L'alignement de la sécurité de l'information sur le business,
- La création d'avantages concurrentiels,
- La réduction des coûts liés aux incidents de sécurité de l'information,
- La protection du patrimoine informationnel de l'organisation,
- L'inspiration de confiance des parties intéressées de l'organisation,
- L'assurance de développements sécurisés pour les clients,
- La protection de l'image de marque,
- Le respect des obligations légales et réglementaires,
- La protection des données (internes/externes/confiées aux tiers, etc.),
- L'assurance d'une reprise de son activité efficiente.

La mise en œuvre de la démarche de sécurité décrite dans la présente politique implique de maîtriser l'ensemble des risques de chaque direction, de définir et contrôler la protection des données, de contrôler et auditer régulièrement les mesures organisationnelles et techniques mises en place pour assurer la sécurité. Elle implique également de maitriser la sécurité de chaque ressource et, en production, de maîtriser le paramétrage de la sécurité et le contrôle des accès à chaque ressource.

Au sein de XXX, le responsable de la sécurité nommé par la direction générale est le garant de la sécurité des systèmes d'information.

Il peut être appuyé dans ce rôle par d'autres responsables de domaines.

1.3. OBLIGATIONS LEGALES ET REGLEMENTAIRES

Il est rappelé que tout collaborateurs doit respecter l'ensemble des lois qui ont vocation à s'appliquer à l'utilisation des moyens informatiques, et notamment celles relative à :

- La protection des données à caractère personnel (loi n°78-17 du 06.01.1978 modifiée, dite « Informatique et libertés »),
- RGPD (Règlement Général sur la Protection des Données) – applicable à depuis le mai 2018, et entré en vigueur le 24 mai 2016 par le Parlement Européen.
- La protection des libertés individuelles (articles 226-1, 226-2, 226-10, 226-13 et 226-16 du code pénal),
- L'atteinte aux mineurs (article 227-23 et 227-24 du code pénal),
- L'apologie du terrorisme, provocation raciale, négationnisme, diffamation et injure (articles 23, 24, 24bis, 30 à 33 de la loi n° du 29 juillet 1881 sur la liberté de la presse),
- Le secret des correspondances (articles 226-15 et 432-9 du code pénal),
- L'escroquerie et fraude informatique (article 313-1, 323-1 et 323-7 du code pénal),
- La contrefaçon (articles L122-6, L122-6-1, L335-2 et L335-3 du code de la propriété intellectuelle).

1.4. PERIMETRE D'APPLICATION DE LA PGSI

La présente politique s'adresse à l'ensemble des entités du groupe XXX. Elle est applicable à tous les collaborateurs, internes et externes du groupe. Dans le cas où celle-ci enfreindrait les lois et/ou règlements des pays dans lesquels XXX est implanté, des PSI locales seront alors déclinées.

Le Groupe XXX est constitué de plus de 2500 collaborateurs qui sont répartis en à travers les régions suivantes :

- XXX
- XXX
- XXX

Elle couvre notamment la gouvernance de la sécurité des systèmes d'information, les composants constituants ces systèmes d'information, leur exploitation et leur maintien en condition de sécurité, leurs accès ainsi que les informations qu'ils traitent, leur sécurité physique et environnementale, la sécurité de l'usage qui en est fait ainsi que celui des données qu'ils traitent.

Par systèmes d'information, la présente PGSI comprend la totalité des moyens organisationnels, matériels et logiciels du Groupe, visant à créer, acquérir, traiter, stocker, archiver, transmettre ou détruire de l'Information. Elle adresse donc en particulier les composants suivants :

+ Les systèmes informatiques de gestion,

+ Les applications institutionnelles (messagerie, bureautique, applications et publications Internet, stockage, sauvegarde…) et celles propres aux activités (applications développées, traitement des données, outils de développement, base de données, etc.),

+ Les interconnexions entre les agences, les clients, les fournisseurs d'accès, hébergeur, franchisés.

1.5. EVOLUTION, VALIDATION ET DIFFUSION DE LA PGSI

La présente PGSI sera à diffusion restreinte seulement pour l'ensemble des collaborateurs de XXX. Elle est consultable EMPLACEMENT. Les différents référentiels sont aussi publiés à cet emplacement.

Le responsable de la sécurité de l'information a la charge du contenu de la PGSI et de son évolution. La Direction Générale a la charge de l'approbation du contenu. Enfin, le service communication de XXX se charge de la diffusion de la PGSI.

Par ailleurs, le canal principal de communication sera la messagerie électronique XXX.

Une adresse électronique (XXX) est mise en place afin d'alerter la Cellule Sécurité des systèmes d'information en cas de problèmes de type email frauduleux, incidents etc.

La sécurité de l'information est évolutive et doit intégrer les changements d'origine :

Externe aux systèmes d'information du groupe XXX:

- Évolution législative et réglementaire,
- Évolution de l'environnement économique et des partenaires,
- Évolution des enjeux et des menaces, quelle que soit leur nature,
- Évolution des technologies,
- Évolution des métiers du groupe XXX.

Interne aux systèmes d'information du groupe XXX:

- Évolution de la compréhension et de l'adhésion du personnel à la sécurité de l'information,
- Évolution des infrastructures et des ressources,
- Prise en compte des retours d'expériences.

La prise en compte de ces différentes évolutions au niveau de la politique de sécurité garantit son efficacité dans le temps et son applicabilité.

La présente politique sera revue en profondeur tous les 3 ans et maintenu à jour tel que prévu par le présent document.

Elle doit aussi prendre en compte les changements ou évolutions majeures affectant les systèmes d'information et leurs environnements (réorganisation du groupe, changement de stratégie, changements législatifs ou réglementaires, intégration de la sécurité dans les contrats clients ou franchisés, etc.).

II. ENJEUX ET BESOINS DE SECURITE

2.1. ENJEUX STRATEGIQUES DU GROUPE

Le positionnement du groupe XXX au niveau national confère un caractère stratégique à la protection de l'information ainsi qu'à de son patrimoine technique et informationnel.

La sécurité des systèmes d'information (SSI) s'impose comme une composante essentielle de la protection du groupe XXX.

Bien que cela soit difficile à évaluer, l'insécurité a un coût qui se manifeste lors d'incidents ou de dysfonctionnements.

Face aux risques encourus, et dans le contexte fonctionnel et organisationnel propre à l'organisme, il convient d'identifier ce qui doit être protégé, de quantifier l'enjeu correspondant, de formuler des objectifs de sécurité et d'identifier, arbitrer et mettre en œuvre les mesures de sécurité adaptées au juste niveau de sécurité retenu.

Cela passe prioritairement par la définition et la mise en place au sein du Groupe XXX d'une « Politique globale de la sécurité de l'information » (PGSI). Les principaux risques relatifs au business du Groupe XXX sont identifiés lors d'une phase d'analyse des activités métier :

- Les risques liés à l'INDISPONIBILITÉ des informations et des systèmes les traitant (intrusion, vol, destruction, panne, déni de service),
- Les risques de DIVULGATION (perte de confidentialité), qu'ils soient accidentels ou volontaires,
- Les risques d'ALTÉRATION (perte d'intégrité).

La PGSI relève d'une vision stratégique de l'organisme et traduit un engagement fort de la direction générale. Elle s'inscrit nécessairement sur le long terme.

Elle est conforme aux dispositions législatives et réglementaires et elle est cohérente avec les politiques de sécurité des organismes partenaires et de ses clients.

Les enjeux essentiels liés à la sécurité de l'information que le groupe XXX s'efforce de mettre en œuvre sont les suivants :

- La protection des données opérationnelles, personnelles, dans les projets internes et les projets clients,
- La protection des fonctions et outils informatiques du groupe,

- La protection des données personnelles relevant des ressources humaines (administration, gestion, etc.).

- Eléments clés BS à ajouter

2.2. CRITERES DE SECURITE

La PGSI du groupe XXX, ainsi que les documents de référence (les normes ISO 2700x, la méthode EBIOS RM de l'ANSSI, etc.…) présentent les bonnes pratiques à appliquer.

Les critères de sécurité (DIC) utilisés dans le cadre de cette politique sont les suivants :

- **Disponibilité** : Propriété d'accessibilité au moment voulu des données et des fonctions par les utilisateurs autorisés. Un niveau contextualisé et encadré doit garantir la disponibilité des données de XXX en fonction des besoins.

  Le besoin de disponibilité de l'information et des fonctions d'un système d'information dépend de la finalité de ce système. Selon la disponibilité requise, les réponses possibles sont variées et peuvent être plus ou moins lourdes à mettre en œuvre. La CSSI est libre, sur la base d'une analyse de risques, d'adopter des niveaux spécifiques de disponibilité correspondant à ses contraintes métier.

- **Intégrité** : « L'intégrité est la prévention d'une modification non autorisée de l'information » norme ISO 7498-2 (ISO90). Ce besoin d'intégrité est par défaut à considérer important dans l'ensemble des systèmes d'information. La CSSI traitement est libre, sur la base d'une analyse de risques, d'adopter des niveaux spécifiques d'intégrité correspondant à ses contraintes métier.

- **Confidentialité** : « La confidentialité est la propriété qu'une information n'est ni disponible ni divulguée aux personnes, composantes ou processus non autorisés » norme ISO 7498-2 (ISO90). Les besoins en confidentialité de l'information doivent être déterminés en cohérence avec leurs natures et la nécessité pour un individu d'y accéder.

III. ANNEXES

3.1. REFERENTIEL DOCUMENTAIRE

- CHARTE DE BON USAGE DES RESSOURCES INFORMATIQUES
- CHARTE DE SECURITE INFORMATIQUE
- CHARTE DEDIEE AUX ADMINISTRATEURS (TECHNIQUES ET FONCTIONNELS)
- CHARTE DU DEVELOPPEUR
- CHARTE UTILISATEUR
- INTEGRATION DE LA SECURITE DANS LES PROJETS SI
- LETTRE D'ENGAGEMENT
- METHODE D'ANALYSE DE RISQUES
- PLAN D'ASSURANCE SECURITE
- PLAN DE SECOURS INFORMATIQUE
- PLAN REPRISE D'ACTIVITE
- POLITIQUE DE GESTION DES MOTS DE PASSE
- POLITIQUE DE TELETRAVAIL
- PROCEDURE DE CLASSIFICATION
- REFERENTIELS DE LA SECURITE DANS LES DEVELOPPEMENTS
- REGLEMENT INTERIEUR
- REGLES D'USAGES DES TELEPHONES MOBILES
- ETC…

3.2. GLOSSAIRE

Abréviation	Définition
CIL	Correspondant Informatique et Libertés
CNIL	Commission Nationale de l'Informatique et des Libertés
CSSI	Cellule de Sécurité des Systèmes d'Information
DF	Direction Financière
DG	Direction Générale
DI	Direction Informatique
DIC	Disponibilité, Intégrité, Confidentialité
DPO	Délégué de Protection des Données (Data Protection Officer)
DRH	Direction des Ressources Humaines
DSI	Direction des Systèmes d'Information
RGPD/GDPR	Règlement Général sur la Protection des Données (General Data Protection Regulation)
IT	Technologies de l'Information (Information Technology)
MOA	Maitrise d'ouvrage
MOE	Maitrise d'œuvre
PAS	Plan d'Assurance Sécurité
PGSI	Politique Globale de Sécurité de l'Information
PRA	Plan de Reprise d'Activité
PTS	Politique Technique de Sécurité
RACI	Matrice « Responsable Approuve Consulté Informé »
RPRA	Responsable du Plan de Reprise d'Activité
RSSI	Responsable de la Sécurité des Systèmes d'Information
SI	Systèmes d'Information
SMSI	Système de Management de la Sécurité de l'Information
SSI	Sécurité des Systèmes d'Information