****

Politique de Sécurité des Systèmes d’Information (PSSI)

Document d’orientation de la sécurité des systèmes d’information

# Contexte et objectifs

L’entreprise {NOM\_ENTREPRISE} évolue dans le secteur {SECTEUR\_ACTIVITE}. Fondée en {ANNEE\_FONDATION}, elle rassemble aujourd’hui plus de {NOMBRE\_EMPLOYES} collaborateurs répartis sur {NOMBRE\_SITES} sites en {ZONE\_GEOGRAPHIQUE}. Elle se distingue par son engagement envers l’innovation et la qualité, et par une approche axée sur la satisfaction client. Cette orientation stratégique a permis à {NOM\_ENTREPRISE} de se positionner comme un acteur clé dans son domaine.

Les systèmes d'information de {NOM\_ENTREPRISE} soutiennent l’ensemble des activités de l’organisation, de la gestion des opérations quotidiennes à la relation client, en passant par la recherche et le développement. La sécurité de ces systèmes est un enjeu central pour préserver la confidentialité, l'intégrité et la disponibilité des données critiques.

**Engagement en Sécurité :**

La **Politique de Sécurité des Systèmes d'Information** (PSSI) de {NOM\_ENTREPRISE} vise à :

* **Assurer la confidentialité** : protéger les données sensibles de l’entreprise et des clients ;
* **Garantir l'intégrité** : veiller à ce que toutes les informations soient exactes et fiables ;
* **Maintenir la disponibilité** : assurer un accès continu aux systèmes et services critiques.

La mise en œuvre de cette politique repose sur un ensemble de processus et de dispositifs techniques et organisationnels, adaptés aux besoins spécifiques de {NOM\_ENTREPRISE}.

**Localisation** : {ZONE\_GEOGRAPHIQUE}  
Les infrastructures de {NOM\_ENTREPRISE} sont réparties sur {NOMBRE\_SITES} sites, interconnectés via un réseau sécurisé, garantissant une communication fluide et sécurisée entre toutes les entités de l’entreprise.

## Périmètre de la SSI

La sécurité des systèmes d’information englobe l'ensemble des infrastructures numériques, incluant les réseaux internes, les postes de travail, les applications métiers et les systèmes critiques de {NOM\_ENTREPRISE}.

* Inventaire
* Inventaire
* Inventaire

## Besoins de sécurité

La sécurité du Système d'Information de {NOM\_ENTREPRISE} repose sur les critères suivants :

**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). Ce principe garantit que seules les personnes ayant l’autorisation nécessaire ont accès aux données sensibles de {NOM\_ENTREPRISE}.

**Disponibilité** : La disponibilité se traduit par l'accessibilité des données et des fonctions au moment voulu pour les utilisateurs autorisés. Cela permet d'assurer que les opérations essentielles de {NOM\_ENTREPRISE} peuvent se dérouler sans interruption, même en cas d'incident.

**Intégrité** : « L’intégrité est la prévention d’une modification non autorisée de l’information » (norme ISO 7498-2). L'intégrité garantit que les données traitées par le Système d'Information restent exactes et fiables, sans altérations non autorisées.

Ces besoins de sécurité s'appliquent aussi bien aux ressources du Système d'Information (postes informatiques, réseaux, applications…) qu'aux données qu'elles traitent. Il est impératif d'inventorier et de classifier ces données (par exemple, données de gestion, scientifiques, nominatives, stratégiques) afin de déterminer leur degré de sensibilité et de mettre en place le niveau de protection approprié.

## Menaces

Afin de mettre en place les moyens de sécurité adéquats, la méthode EBIOS préconise de connaître les typologies de menaces et leurs impacts. On distingue ainsi :

* **Les attaques visant directement le système d’information** : Ces attaques peuvent inclure le vol de données (et éventuellement des ressources supportant ces données), la modification des données, le déni de service, etc.
* **Les attaques visant les ressources informatiques** : Cela inclut le vol de ressources, le détournement des ressources, l’altération des données et l’émission de logiciels malveillants (malware).
* **Les accidents** : Il s'agit des sinistres naturels, de l’altération accidentelle des données ou des ressources.

Pour chaque menace, il est nécessaire d’en évaluer le risque, c’est-à-dire de considérer la probabilité que celle-ci devienne réalité et de détecter les éventuels facteurs aggravants tels que la négligence constatée, l’insuffisance d’information ou de consignes.

## Pilotage

Au sein de {NOM\_ENTREPRISE}, la responsabilité générale de la sécurité des systèmes d’information relève de <Titre du responsable principal, ex. Directeur Général> en tant qu’<Titre officiel, ex. Autorité Qualifiée pour la Sécurité des Systèmes d’Information (AQSSI)>. Il est assisté dans cette fonction par le Responsable de la Sécurité des Systèmes d’Information (RSSI), qui peut également remplir des fonctions supplémentaires selon les besoins de l'entreprise.

La PSSI de {NOM\_ENTREPRISE} s’inscrit dans le cadre de la politique et des directives émanant de <Nom de l'organisme ou autorité externe en charge de la SSI, ex. Direction Centrale de la Sécurité des Systèmes d’Information (DCSSI)>. Ces directives peuvent être relayées par des entités sectorielles telles que <Exemples d'organismes ou de ministères concernés> pour assurer la conformité et la coordination des pratiques de sécurité.

Le pilotage courant de la sécurité est sous la responsabilité du RSSI et, le cas échéant, de son adjoint. La mise en œuvre opérationnelle est confiée au RSSI et à son équipe pour le contrôle des flux de données entrants et sortants ainsi que pour la gestion des ressources informatiques et multimédias. Les responsables hiérarchiques de chaque département ou division (par exemple, les directeurs ou chefs de service) sont responsables de la sécurité des systèmes d'information dans leur périmètre respectif.

## Coordination avec les autres tutelles

Les dispositions contractuelles qui régissent la tutelle de {NOM\_ENTREPRISE} incluent des clauses relatives à la sécurité des systèmes d’information, définissant en particulier les responsabilités respectives.Ces dispositions peuvent être formalisées dans des contrats pluriannuels, tels que des contrats de collaboration ou des conventions de partenariat. Ce document définit la PSSI de référence pour l’entité ou l’unité concernée.

En tant que responsable de la SSI de {NOM\_ENTREPRISE}, le directeur ou le responsable désigné :

* s’assure que les documents de PSSI de son unité (ex. charte de sécurité, gestion des traces) sont alignés avec ceux de toutes les tutelles et partenaires (ex. noms des organismes partenaires tels que CNRS, EPST, etc.);
* désigne un Correspondant de la Sécurité des Systèmes d’Information (CSSI) pour son unité, qui agit comme point de contact pour les autres tutelles. Le CSSI est intégré aux chaînes fonctionnelles de chaque tutelle et assure les échanges d’information nécessaires.

En cas d’incident, le traitement est assuré par la voie fonctionnelle de la tutelle responsable, tout en veillant à informer les autres partenaires impliqués. Si nécessaire, une concertation peut avoir lieu pour décider des mesures à prendre, y compris le dépôt de plainte.

# 2. Mise en œuvre de la PSSI

La PSSI de {NOM\_ENTREPRISE} établit un ensemble de principes d'ordre organisationnel et technique prioritaires. Ces principes visent à encadrer la sécurité des systèmes d'information et à soutenir la stratégie globale de l'entreprise. Ils sont explicités et peuvent être complétés par des instructions ou des dispositions techniques spécifiques. La responsabilité de leur élaboration, diffusion et communication revient à la chaîne fonctionnelle SSI de l'entreprise, comprenant le RSSI et les équipes de sécurité désignées.

## Organisation ‐ Responsabilités

### Responsabilité des différents acteurs

Les acteurs impliqués dans la sécurité des systèmes d’information de {NOM\_ENTREPRISE} doivent être clairement informés de leurs responsabilités en matière de SSI. Dans l'exercice de leurs fonctions, ils doivent respecter leur devoir de réserve et, le cas échéant, se conformer à des obligations de secret professionnel.

Le Directeur Général, le Secrétaire Général, le Responsable de la Sécurité des Systèmes d’Information (RSSI), et son adjoint peuvent être soumis à des habilitations particulières, telles que des habilitations de niveau "confidentiel défense" ou équivalent, selon les besoins de l'entreprise et la sensibilité des données traitées.

### Responsable de la Sécurité des Systèmes d’Information

Le Responsable de la Sécurité des Systèmes d’Information (RSSI) de {NOM\_ENTREPRISE} exerce sous l’autorité directe de <Titre du responsable supérieur, ex. Directeur Général>. Les activités principales du RSSI incluent :

* Contribuer activement à l’élaboration et à la mise en œuvre d’une politique de sécurité cohérente, acceptée par l'ensemble des parties prenantes.
* Examiner et valider tous les projets de l’entreprise afin de s'assurer que les éléments technologiques nécessaires à l’application de la PSSI soient intégrés.
* Coordonner et animer le réseau des correspondants en sécurité de l’entreprise, assurant ainsi la cohérence et la communication au sein des équipes.
* Exploiter et relayer les informations pertinentes sur la sécurité provenant de sources externes telles que <Exemples de sources pertinentes pour l'entreprise, ex. CERT nationaux, organismes de cybersécurité>.
* Promouvoir et faire respecter la charte déontologique ainsi que la charte d'utilisation des moyens informatiques et des réseaux de l'entreprise.
* Proposer et mettre en œuvre des actions de sensibilisation et d’information pour tous les utilisateurs concernant la sécurité des systèmes d’information.
* Être l’intermédiaire direct entre <Nom du responsable supérieur, ex. le Directeur Général> et les autorités compétentes en cas de problème.

### Accès aux ressources informatiques

La mise à disposition des moyens informatiques pour un utilisateur (employé, consultant, partenaire) doit être formalisée lors de l'arrivée, des changements de poste, et du départ de l'utilisateur. L'accès aux ressources doit être contrôlé via des procédures d'identification et d'authentification, et doit être adapté en fonction des droits et privilèges associés au profil de l'utilisateur.

### Charte informatique

Avant de recevoir l'accès aux outils informatiques, chaque utilisateur doit être informé des droits et des devoirs qui accompagnent la mise à disposition de ces outils. Cette information est transmise à travers la « charte de bon usage des moyens informatiques » intégrée dans le règlement interne de {NOM\_ENTREPRISE}.

### Cyber surveillance

Pour garantir la sécurité des systèmes d'information, il est nécessaire de surveiller le trafic réseau et de tracer les actions effectuées. Les dispositifs de surveillance doivent être conformes à la réglementation en vigueur et respecter les principes de proportionnalité (adéquation entre les moyens et l'enjeu de la sécurité) et de transparence (information des employés et des parties prenantes sur ces dispositifs).

## Protection des données

### Disponibilité, confidentialité et intégrité des données

Le traitement et le stockage des données numériques, l’accès aux applications et aux services, ainsi que les échanges de données entre systèmes d’information doivent être réalisés en suivant des méthodes qui préviennent la perte, la modification, l’utilisation abusive ou la divulgation non autorisée des données sensibles.

Des sauvegardes régulières des données, accompagnées de processus de restauration validés, doivent être mises en place. On distingue :

* Les **sauvegardes de production** : pour la restauration rapide de données spécifiques.
* Les **sauvegardes de recours** : pour la reprise des services sur des infrastructures externes en cas d’incident majeur.

Une analyse approfondie de la criticité et des caractéristiques des données (ex. volatilité, fluctuations) permet de définir la fréquence et le type de sauvegarde ainsi que la durée de rétention, tout en respectant les législations en vigueur.

### Protection des données sensibles

Le stockage et la transmission de données considérées comme « sensibles » nécessitent l'utilisation de moyens spécifiques et agréés aux normes nationales et internationales. L'habilitation seule ne suffit pas pour accéder à un document sensible ; il est également nécessaire de justifier d'un besoin d’en connaître dans le cadre de ses fonctions.

Les données non classifiées, mais présentant un caractère sensible, doivent être identifiées et, si nécessaire, étiquetées selon un niveau de sensibilité approprié. Une évaluation régulière de la sensibilité des données doit être réalisée afin d’adapter les mesures de protection. Ces données doivent être protégées par des contrôles d’accès stricts (authentification et autorisation), et des mesures de chiffrement pour leur stockage et leur échange, garantissant ainsi leur confidentialité.

Avant la cession ou la mise au rebut d’un matériel contenant des données sensibles, il est impératif de vérifier que toutes les données ont été effacées selon des méthodes efficaces et conformes aux recommandations techniques nationales. Si cela s’avère impossible, les supports concernés doivent être détruits de manière sécurisée.

### Données à caractère personnel

Les traitements de données susceptibles de contenir des informations à caractère personnel (conformément à la loi applicable, ex. la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés) doivent faire l’objet des formalités de déclaration ou de demande d'autorisation auprès de l'autorité compétente, ex. la CNIL, via le délégué à la protection des données (DPO).

Les données à caractère personnel sont considérées comme sensibles et doivent, à ce titre, faire l’objet de mesures de protection rigoureuses, incluant le chiffrement, des contrôles d’accès renforcés et des processus de gestion des incidents de sécurité adaptés.

### Chiffrement

Le chiffrement est un moyen de protection essentiel, obligatoire pour le stockage et l’échange de données sensibles. Les produits matériels et logiciels utilisés doivent être certifiés ou agréés par l'organisme compétent, ex. l’ANSSI ou toute autre autorité nationale/internationale. Une copie des clés permettant de déchiffrer les données doit être conservée dans un emplacement sécurisé et distinct, garantissant l’accès en cas de besoin.

## Sécurisation du Système d’information

### Administration des serveurs

L’administration des serveurs de {NOM\_ENTREPRISE} est placée sous la responsabilité des administrateurs systèmes et réseaux de <nom du service ou département informatique>. Pour les serveurs situés au sein des différentes composantes de l'entreprise, l’administration relève des administrateurs systèmes et réseaux responsables de ces composantes.

### Administration des postes de travail

L’administration des postes de travail individuels au sein de {NOM\_ENTREPRISE} est sous la responsabilité des administrateurs systèmes et réseaux de <nom de la division ou département>. L'administration des postes par les utilisateurs eux-mêmes doit rester une exception, justifiée par des besoins spécifiques et des compétences adéquates.

Les administrateurs systèmes et réseaux de l’entreprise peuvent intervenir à distance pour effectuer des opérations de maintenance sur le poste de travail d’un utilisateur, après en avoir été informé et en respectant les réglementations en vigueur, telles que celles définies par la législation sur la protection des données personnelles et la confidentialité.

### Sécurisation des postes de travail et des moyens nomades

La sécurisation des postes de travail et des moyens nomades au sein de {NOM\_ENTREPRISE} est sous la responsabilité des administrateurs systèmes et réseaux de <nom de la division ou service>. L’accès à ces postes doit être protégé par des mots de passe suffisamment robustes ; chaque mot de passe est personnel et confidentiel et ne doit pas être divulgué ou laissé sans protection.

Les utilisateurs sont tenus de s'assurer du bon fonctionnement des outils de sécurisation installés sur les dispositifs informatiques mis à leur disposition, y compris les mises à jour régulières de l’antivirus, du système d’exploitation et des applications. Ils doivent signaler tout dysfonctionnement ou incident au correspondant sécurité désigné ou au service IT de l'entreprise.

En particulier, des mesures spécifiques doivent être prises par les utilisateurs lors de l’utilisation des moyens nomades en dehors de leur zone de sécurité habituelle, comme la protection contre le vol et le chiffrement des données sensibles.

### Contrôle d’accès

Tout accès aux systèmes d’information de {NOM\_ENTREPRISE} est soumis à l'identification et à l'authentification des demandeurs, ainsi qu'au contrôle de leurs autorisations et habilitations. L'authentification doit, dans la mesure du possible, s'effectuer via un annuaire centralisé ou un système de gestion d'identités utilisé par l'entreprise. Il est crucial de définir précisément les autorisations et de limiter les privilèges à ce qui est strictement nécessaire. Les accès doivent être journalisés pour assurer une traçabilité complète. L’utilisation de comptes partagés ou anonymes doit rester une exception, justifiée par des besoins spécifiques.

L'attribution et la modification des accès et des privilèges à un service doivent être validées par le propriétaire de ce service. Pour les services sensibles, un inventaire régulier des accès doit être effectué et mis à jour.

### Sécurité des applications

La sécurité doit être intégrée à toutes les phases d’un projet, qu'il soit interne ou externe, lié au système d’information de l’entreprise. Chaque projet doit être accompagné d’un dossier de sécurité décrivant les objectifs, les méthodes et les mesures recommandées. En particulier, les applications métiers et les applications web doivent être conçues en cohérence avec la sensibilité des données qu'elles manipulent.

Chaque dossier de sécurité doit être validé par le RSSI ou par le comité de sécurité désigné, selon l'importance de l'application.

### Infogérance et télémaintenance externes

L’infogérance implique que des sociétés extérieures, mandatées pour gérer une partie des services informatiques de {NOM\_ENTREPRISE} ou de ses composantes, aient accès au système d’information, que ce soit depuis l’extérieur ou l’intérieur des locaux. Un contrat doit être établi entre l'entreprise et chaque société prestataire, spécifiant clairement les droits d’accès, les engagements de responsabilité et les mesures d’imputabilité en cas d’incident.

Des mécanismes permettant de s’assurer du respect des limites d’intervention doivent être mis en place autant que possible. Ces mécanismes incluent des processus de surveillance des accès et des vérifications régulières des audits de conformité.

L'externalisation de la gestion de composants critiques pour le système d'information doit être évitée, sauf si des garanties spécifiques sont prévues et validées par le RSSI ou un comité de sécurité ou un responsable de haut niveau de l'entreprise, selon la criticité et l'importance de l'application.

### Réseau

L’administration du réseau de {NOM\_ENTREPRISE} est sous la responsabilité exclusive de <nom du service ou de la mission réseau>. Sur les sites distants, cette responsabilité peut être déléguée aux administrateurs systèmes et réseaux des unités ou composantes concernées.

Les systèmes d’information doivent être protégés contre les menaces extérieures à l'aide de filtres d'accès configurés sur les équipements en tête de réseau. Ces filtres doivent s'appliquer aussi bien aux flux entrants qu'aux flux sortants. Les flux entrants se rapportent principalement à l’accès aux serveurs depuis le réseau interne de {NOM\_ENTREPRISE} ou depuis l'extérieur. L'accès externe aux postes de travail doit rester exceptionnel et être justifié par des besoins précis et des compétences adéquates.

La politique de filtrage des accès doit suivre le principe de « tout ce qui n’est pas explicitement autorisé est interdit ». Les serveurs doivent être protégés spécifiquement des postes de travail et des autres serveurs, avec une distinction entre ceux accessibles uniquement depuis le réseau interne et ceux ouverts à l'extérieur. Pour chaque catégorie de serveur, les filtres d’accès, tant pour les flux entrants que sortants, doivent être configurés selon la règle de « tout ce qui n’est pas explicitement autorisé est interdit ».

Les serveurs accessibles depuis l’extérieur doivent faire l’objet d’une surveillance renforcée, comprenant l'utilisation d'outils d'analyse des traces et de métrologie. L'accès externe aux serveurs via des dispositifs nomades de {NOM\_ENTREPRISE} doit se faire via des connexions dédiées et chiffrées (VPN).

L'accès au réseau sans fil doit être contrôlé spécifiquement et limité aux utilisateurs authentifiés. Les connexions doivent être journalisées pour garantir une traçabilité complète. Une vigilance particulière doit être exercée lors de la reconnexion des dispositifs nomades sur le réseau interne pour éviter l'introduction de logiciels malveillants.

### Maintien du niveau de sécurité

Le maintien du niveau de sécurité doit faire l'objet de dispositions techniques sous la responsabilité du RSSI. Ces dispositions doivent inclure le suivi et le maintien de l'état de sécurité des équipements et infrastructures : application de correctifs, mises à jour régulières des antivirus, des pare-feu, etc.

Elles doivent également préciser les conditions de surveillance continue du fonctionnement du système d’information pour garantir son état de sécurité, notamment par l'analyse des journaux d'activités, la vérification des vulnérabilités connues, et le suivi des avis de sécurité publiés par des sources fiables. Des processus d'audit et des tests réguliers doivent être planifiés pour s'assurer que les mesures de sécurité restent efficaces et adaptées aux évolutions des menaces.

## Mesure du niveau effectif de sécurité

### 2.4.1 Contrôle de gestion

Le contrôle de gestion de la sécurité des systèmes d’information est sous la responsabilité du RSSI et de <titre de l'autre responsable, ex. Directeur de la sécurité ou FSD>. Ce contrôle doit donner lieu à la création et à la mise à jour régulière d’un tableau de bord de la SSI, permettant un suivi précis des indicateurs de performance et des incidents de sécurité.

### Audits

Le niveau de sécurité des systèmes d’information et la conformité de la mise en œuvre des recommandations doivent faire l'objet d'audits réguliers. Ces audits peu vent être internes, sous la responsabilité du RSSI, ou externes, réalisés sous la supervision du RSSI et avec l'approbation de <titre du responsable de l'entreprise, ex. Directeur Général ou comité de sécurité>.

Ces audits permettent de s'assurer de l'efficacité des mesures de sécurité en place et de leur conformité aux normes et aux meilleures pratiques du secteur.

### Journalisation, tableaux de bord

Le système d’information de {NOM\_ENTREPRISE} doit intégrer des dispositifs de journalisation centralisés et sécurisés pour assurer la protection et l’utilisation correcte des services. L'objectif est de détecter les intrusions ou les usages frauduleux, d'identifier les causes et origines des incidents, et d'éviter toute contamination d'autres systèmes pour permettre un rétablissement rapide.

Conformément aux réglementations en vigueur, ces informations peuvent être transmises aux autorités compétentes avec l’accord du <titre du responsable concerné, ex. Directeur Général ou RSSI>. La durée de conservation des fichiers de traces à des fins de preuve doit être conforme aux lois et règlements applicables.

Il est essentiel de définir et de communiquer aux utilisateurs les règles d'exploitation des fichiers de traces, incluant leur contenu, leur durée de conservation et leur usage, tout en respectant le « principe de proportionnalité » et les exigences légales concernant le traitement des informations à caractère personnel.

### Les fichiers de traces

Les fichiers de traces doivent être systématiquement analysés pour détecter d’éventuels problèmes et pour produire des statistiques et des tableaux de bord de suivi. Des mécanismes automatisés et des audits réguliers peuvent être mis en place pour garantir l’efficacité de ces analyses.

### Posture de sécurité

En matière de sécurité des systèmes d’information, le niveau normal des recommandations internes de la SSI correspond aux directives <préciser les niveaux de sécurité, ex. « jaune » et « orange »> du plan de sécurité global de l'entreprise. Ces recommandations doivent être régulièrement révisées et rappelées par le RSSI ou <autre responsable pertinent>.

Les dispositions internes doivent permettre une réactivité suffisante en cas de passage à un niveau d'alerte plus élevé. Des exercices de simulation et des tests réguliers peuvent être prévus pour évaluer la capacité de l'entreprise à répondre aux menaces accrues et à appliquer les mesures recommandées.

### Mises en garde

L'utilisation de certains matériels ou logiciels peut présenter des risques pour la sécurité des systèmes d'information. Ces produits font l’objet de « mises en garde » émises par <les responsables ou équipes SSI, ex. RSSI, équipes de sécurité>, et peuvent inclure des recommandations spécifiques d'utilisation, voire des interdictions pures et simples pour garantir la protection des systèmes d'information.

### Gestion d’incidents

Chaque acteur du système d’information, qu’il soit utilisateur ou administrateur, doit être sensibilisé à l'importance de signaler tout incident réel ou suspecté. Cela inclut le vol de données, l’utilisation abusive des systèmes ou des supports de données. Le signalement des incidents à la chaîne fonctionnelle SSI et aux autorités hiérarchiques doit être systématique.

Lorsque l’incident peut affecter une composante ou le fonctionnement de {NOM\_ENTREPRISE}, le RSSI doit être immédiatement informé et, selon la gravité de l'incident, le dirigeant de l'entreprise ou un comité de gestion de crise peut être informé en parallèle. Si l'incident concerne des données sensibles ou des systèmes critiques, le RSSI, en accord avec la direction, peut notifier les autorités compétentes (ex. autorités de régulation, organismes de cybersécurité).

Toute infraction susceptible d’avoir des implications juridiques doit faire l'objet d'une plainte déposée par le RSSI, après consultation et approbation par la direction générale ou le conseil exécutif de l'entreprise.

Dans le cas de collaborations ou de partenariats impliquant d'autres entités, il est essentiel d'informer les partenaires et, le cas échéant, de coordonner la réponse avec eux.

Les données statistiques sur la gestion des incidents doivent être intégrées au tableau de bord de la SSI pour assurer un suivi précis et favoriser l'amélioration continue des processus de sécurité.

### Gestion de crise

<Nom de l'Entreprise> doit prévoir un dispositif organisationnel spécifique pour gérer les crises de nature informatique. Ce dispositif intègre les risques liés aux incidents informatiques et leurs impacts potentiels sur la sécurité des systèmes d’information. Le RSSI ou un comité de gestion de crise doit être informé dès le déclenchement d’une crise ayant des implications sur la sécurité des systèmes d’information. Il est de la responsabilité du RSSI de coordonner la communication avec les parties concernées, telles que les équipes de direction, les partenaires stratégiques et, si nécessaire, les autorités réglementaires.

### Plan de continuité

Chaque division ou département de {NOM\_ENTREPRISE} doit établir un plan de continuité et les procédures associées. Ce plan doit permettre de maintenir les opérations essentielles dans un mode dégradé et de rétablir progressivement toutes les fonctionnalités du système d’information après un incident.

Dans les cas où l'entreprise travaille en partenariat ou dans des collaborations mixtes, il est important de coordonner ces plans de continuité avec les autres entités impliquées pour garantir une gestion harmonieuse des crises.



# Objet

La présente charte a pour objet de définir les conditions d’utilisation et les règles de bon usage des moyens informatiques de {NOM\_ENTREPRISE} afin de garantir une utilisation responsable et conforme aux lois et règlements en vigueur.

# Domaine d’application

La charte s’applique à l’ensemble des personnes ayant accès aux moyens informatiques de {NOM\_ENTREPRISE}, quel que soit leur statut (employés, prestataires, stagiaires, etc.).

# Moyens informatiques

Sont considérés comme moyens informatiques de {NOM\_ENTREPRISE}, les serveurs, postes de travail, stations de consultation, réseaux internes et externes, ainsi que les ordinateurs personnels des services et départements, les bases de données, le parc logiciel, et les périphériques affectés à ces équipements. Sont également inclus les ressources accessibles par le réseau de l’entreprise et toutes les connexions aux réseaux externes.

# Utilisations

## Finalité de l’utilisation des moyens informatiques de {NOM\_ENTREPRISE}

L'utilisation des moyens informatiques de {NOM\_ENTREPRISE} est limitée aux activités professionnelles, dans le cadre strict des besoins de l’entreprise et de ses missions.

## Autorisations particulières

Toute utilisation des moyens informatiques de {NOM\_ENTREPRISE} à des fins autres que celles prévues doit faire l'objet d'une autorisation préalable délivrée par <le responsable de l'entité ou service compétent>.

## Utilisations prohibées

Il est strictement interdit d’utiliser les moyens informatiques de l’entreprise à des fins contraires aux lois et règlements en vigueur, notamment pour diffuser des idéologies politiques, porter atteinte aux bonnes mœurs, à la dignité ou à la vie privée des personnes.

# Utilisateurs

## Identification des utilisateurs

Un utilisateur désigne toute personne autorisée à accéder aux moyens informatiques de {NOM\_ENTREPRISE}, que ce soit de manière régulière ou occasionnelle, à des fins professionnelles ou non.

## Obligations des utilisateurs

### Règles générales

Les utilisateurs doivent respecter la charte de bon usage des moyens informatiques de {NOM\_ENTREPRISE}. Ils doivent se conformer aux lois et règlements en vigueur ainsi qu’aux règles de courtoisie et de politesse lors de l'utilisation des ressources informatiques. L'accès aux systèmes informatiques doit se faire uniquement dans le cadre des autorisations accordées. Les utilisateurs sont également tenus de suivre les mesures de sécurité prévues par la charte et de se conformer aux directives des responsables informatiques.

### Fichiers des utilisateurs

Les utilisateurs peuvent créer des fichiers privés dont ils ont un accès exclusif. Tant que le créateur ne met pas ces fichiers à disposition du public, ils doivent être considérés comme privés. Toute destruction, altération ou reproduction des fichiers sans autorisation expresse est interdite.

### Préservation des matériels et locaux

Les utilisateurs doivent veiller au bon usage des matériels, logiciels et locaux qui leur sont confiés. En cas de détection d'une dégradation ou d'un dysfonctionnement, ils doivent en informer rapidement le responsable informatique.

### Pénétration non autorisée dans les moyens informatiques

Toute tentative d'accès non autorisé aux moyens informatiques ou de maintien d'accès par un utilisateur est strictement interdite. Il est interdit d’utiliser ou de tenter d’utiliser le compte d’un autre utilisateur. Toute manœuvre visant à masquer l’identité réelle d’un utilisateur ou à accéder aux systèmes sous une fausse identité est également prohibée.

### Utilisation des comptes et des dispositifs de contrôle d’accès

Les utilisateurs doivent prendre toutes les mesures nécessaires pour protéger leurs comptes et dispositifs d'accès contre l'utilisation frauduleuse. Ils doivent notamment :

* Veiller à la confidentialité de leurs codes d’accès, mots de passe, cartes magnétiques, clés ou tout autre dispositif d'accès personnel ;
* Ne pas prêter, vendre ou partager leurs comptes et dispositifs d'accès ;
* Se déconnecter après chaque session de travail, particulièrement lorsqu’ils quittent leur poste ;
* Signaler immédiatement toute tentative d’accès suspecte ou tout dysfonctionnement au RSSI ou au service informatique ;
* Changer régulièrement leurs codes d'accès ;
* S'assurer que les fichiers confidentiels ne soient pas accessibles par des tiers ;
* Informer le RSSI lorsqu'ils ne peuvent pas utiliser leurs comptes pour une période prolongée.

## Responsabilité des utilisateurs

### Responsabilité des utilisations

Les utilisateurs sont responsables de l’usage qu'ils font des moyens informatiques de {NOM\_ENTREPRISE}, ainsi que des informations qu'ils mettent à disposition du public. Ils doivent veiller à une utilisation conforme aux politiques de l'entreprise et aux lois en vigueur.

### Responsabilité des comptes et dispositifs de contrôle d’accès

Les titulaires de comptes ou de dispositifs de contrôle d'accès sont responsables de toutes les actions entreprises, qu'elles soient locales ou distantes, depuis leurs comptes ou sous leur couverture. Ils doivent garantir que l'utilisation de ces dispositifs respecte les autorisations qui leur ont été attribuées.

## Sanctions

En cas de non-respect des obligations, des sanctions peuvent être appliquées conformément aux procédures définies par {NOM\_ENTREPRISE} et décrites à l’article correspondant de la charte ou du règlement interne.

# Responsables informatiques

## Nomination

Les directeurs de départements, divisions ou services de {NOM\_ENTREPRISE} doivent désigner un ou plusieurs responsables informatiques pour chaque site ou unité sous leur responsabilité.

## Fonction des responsables informatiques

Les responsables informatiques sont chargés de :

* Autoriser l’accès aux moyens informatiques ;
* Attribuer et gérer les comptes, mots de passe, cartes magnétiques et autres dispositifs d’accès en accord avec les directives de la direction ;
* Définir les conditions d’utilisation des moyens informatiques en fonction des besoins des utilisateurs et des règles internes de l'entreprise ;
* Informer les utilisateurs des bonnes pratiques et des règles définies dans la charte d’utilisation des moyens informatiques ;
* Garantir le bon fonctionnement et la disponibilité des moyens informatiques.

## Pouvoir des responsables informatiques

Les responsables informatiques ont le droit de surveiller l’usage des moyens informatiques pour lesquels ils sont responsables. Ils peuvent accéder aux fichiers, données et travaux des utilisateurs si nécessaire, dans le cadre de leurs fonctions. Ils sont également habilités à prendre des mesures d’urgence pour assurer la continuité des services et la disponibilité des ressources informatiques.

## Obligations des responsables informatiques

### Confidentialité

Les responsables informatiques doivent préserver la confidentialité des informations et des fichiers auxquels ils ont accès dans le cadre de leurs fonctions.

### Qualité du service

Les responsables informatiques doivent s’efforcer de limiter l'impact de leurs interventions sur les utilisateurs et assurer la disponibilité continue et le bon fonctionnement des moyens informatiques de {NOM\_ENTREPRISE}.

### Information

Les responsables informatiques doivent signaler toute tentative de violation d'accès ou tout incident de sécurité susceptible de mettre en péril les moyens informatiques de {NOM\_ENTREPRISE} au RSSI et <autre responsable pertinent, ex. chef de service informatique ou comité de sécurité>.

### Sécurité

Les responsables informatiques doivent veiller à ce que les codes d'accès choisis par les utilisateurs respectent les exigences de sécurité définies par <l'organisme ou l'équipe responsable de la politique de sécurité, ex. RSSI ou comité de sécurité>.

# Données nominatives

Les traitements automatisés de données nominatives mis en œuvre par {NOM\_ENTREPRISE}, ses divisions ou par tout utilisateur doivent respecter les dispositions de la loi applicable en matière de protection des données personnelles, telle que <la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, ou autre législation équivalente selon le pays>.

# Modification et altération des moyens informatiques

## Modification des environnements

Aucune modification des environnements logiciels, matériels et périphériques de {NOM\_ENTREPRISE} ne doit être effectuée sans l'accord préalable du responsable informatique. Cette règle s'applique même si les modifications ne semblent pas affecter le fonctionnement des systèmes. Par "modification d’environnement", on entend toute action impliquant l'ajout, la suppression ou la configuration de composants pouvant altérer le fonctionnement normal des moyens informatiques.

## Virus, chevaux de Troie, bombes logiques

Il est interdit d’introduire, d’utiliser ou de diffuser tout logiciel ou matériel pouvant nuire aux moyens informatiques, tels que des virus, chevaux de Troie, bombes logiques et autres dispositifs similaires. Toute recherche ou expérimentation liée à ces dispositifs doit être explicitement autorisée par le responsable informatique.

# Conséquences des manquements à la charte et poursuites

## Mesures et sanctions applicables par les responsables informatiques

### Mesures d’urgence

En cas d'urgence, les responsables informatiques de {NOM\_ENTREPRISE} peuvent prendre les mesures suivantes :

* Déconnecter un utilisateur, avec ou sans préavis, en fonction de la gravité de la situation ;
* Isoler ou neutraliser temporairement toute donnée ou fichier qui, en contradiction avec la charte, met en péril la sécurité des systèmes.

### Mesures donnant lieu à information

Sous réserve d’informer le responsable du service ou la direction, les responsables informatiques peuvent :

* Avertir un utilisateur ;
* Limiter provisoirement l'accès d'un utilisateur ;
* Réinitialiser temporairement les codes d'accès ou fermer des comptes ;
* Effacer, confiner ou isoler tout contenu en contradiction avec la charte et pouvant compromettre la sécurité des systèmes ;
* Informer le RSSI de tout incident ou risque détecté ;
* Signaler l'incident à la direction de l'entreprise.

### Mesures soumises à autorisation du directeur ou responsable du service

Sous condition d’autorisation préalable du directeur ou du responsable de service, les responsables informatiques peuvent :

* retirer les codes d’accès ou autres dispositifs de contrôle d’accès et fermer les comptes ;
* interdire à titre définitif à un utilisateur tout accès aux moyens informatiques dont il est responsable.

## Autres sanctions internes

Sans préjudice du pouvoir de sanction des services et départements de {NOM\_ENTREPRISE}, la direction peut appliquer toutes les sanctions internes nécessaires pour assurer le respect de la charte et le bon fonctionnement des services. En particulier, des sanctions disciplinaires peuvent être prises conformément aux procédures internes et aux réglementations applicables à l'entreprise. Ces sanctions ne sont pas exclusives des poursuites civiles ou pénales pouvant être engagées.

## Poursuites civiles et pénales

La direction de {NOM\_ENTREPRISE}, après consultation des instances de gouvernance, peut engager des poursuites civiles contre les utilisateurs en cas de violation grave. Si nécessaire, la direction peut également informer les autorités compétentes, y compris le procureur, des infractions commises par les utilisateurs.