Une image contenant texte, logo, symbole, Police

Description générée automatiquement

Politique de Sécurité des Systèmes

d'Information (PSSI) simplifiée

La présente Politique de Sécurité des Systèmes d'Information (PSSI) établit un cadre essentiel pour la protection de nos données et de nos infrastructures numériques.

Dans un contexte où les menaces cybernétiques évoluent rapidement, il est crucial que notre commune, malgré sa taille modeste, adopte une approche proactive en matière de sécurité informatique.

Ce document s'adresse à l'ensemble de notre personnel municipal, y compris les agents, les élus et les prestataires externes qui ont accès à nos ressources informatiques. Il vise à instaurer une culture de la sécurité, adaptée à nos moyens et à nos besoins spécifiques.

[1. Objectifs 2](#_Toc177234821)

[2. Responsabilités 2](#_Toc177234822)

[3. Règles de base 2](#_Toc177234823)

[3.1 Gestion des accès et authentification 2](#_Toc177234824)

[3.2 Protection des postes de travail 3](#_Toc177234825)

[3.3 Politique de sauvegarde 3](#_Toc177234826)

[3.4 Communication électronique et usage d'Internet 4](#_Toc177234827)

[3.5 Gestion des équipements et mises à jour 4](#_Toc177234828)

[3.6 Utilisation du Wifi 4](#_Toc177234829)

[3.7 Gestion des périphériques amovibles 4](#_Toc177234830)

[3.8 Politique de bureau propre 5](#_Toc177234831)

[3.9 Gestion des accès des prestataires externes 5](#_Toc177234832)

[3.10 Procédure de départ des agents 5](#_Toc177234833)

[3.11 Gestion des incidents 5](#_Toc177234834)

[4. Formation et sensibilisation 6](#_Toc177234835)

[5. Conformité RGPD et protection des données personnelles 7](#_Toc177234836)

[6. Sanctions 7](#_Toc177234837)

[7. Annexes 8](#_Toc177234838)

Dernière mise à jour le xxxxxxxxxxx

# Objectifs

Notre Politique de Sécurité des Systèmes d'Information (PSSI) poursuit plusieurs objectifs fondamentaux.

Tout d'abord, elle vise à garantir la protection des données de nos habitants et de notre commune, préservant ainsi la confiance que nos administrés placent en nous.

Ensuite, elle cherche à assurer la continuité de nos services municipaux, même en cas d'incident informatique, afin de maintenir un service public de qualité.

Par ailleurs, cette politique nous permet de respecter les obligations légales en vigueur, notamment le Règlement Général sur la Protection des Données (RGPD), renforçant ainsi notre crédibilité en tant qu'institution.

Enfin, elle a pour but de sensibiliser l'ensemble de nos utilisateurs aux bonnes pratiques en matière de sécurité informatique, créant ainsi un environnement numérique plus sûr pour tous.

# Responsabilités

La sécurité de nos systèmes d'information est l'affaire de tous, mais elle s'organise selon une chaîne de responsabilités claire.

Le Maire, en tant que représentant légal de la commune, porte la responsabilité ultime de la sécurité des systèmes d'information.

Cette responsabilité se traduit par un engagement fort en faveur de la mise en œuvre et du respect de cette politique.

Au quotidien, chaque agent et élu joue un rôle crucial dans l'application de cette politique. Ils sont les gardiens de nos données et de nos systèmes dans leurs activités quotidiennes.

Le directeur général des services assure la coordination des actions de sécurité informatique. Il est le point de contact pour toutes les questions relatives à la sécurité des systèmes d'information et veille à la cohérence des pratiques au sein de notre commune.

# Règles de base

## Gestion des accès et authentification

La sécurité de nos systèmes d'information repose en grande partie sur une gestion rigoureuse des accès.

Chaque utilisateur est responsable de la protection de ses identifiants. Il est impératif d'utiliser des mots de passe robustes, longs (au moins 12 caractères) et uniques pour chaque compte, et de ne jamais les partager, même avec des collègues de confiance.

Contrairement aux anciennes pratiques, il n’est plus recommandé de changer périodiquement les mots de passe, car cela peut conduire à l'utilisation de mots de passe plus faibles ou à leur réutilisation.

En revanche, les mots de passe doivent être immédiatement modifiés en cas de suspicion de compromission.

La mise en place de la double authentification renforce considérablement la sécurité de nos comptes. Pour faciliter la gestion de multiples mots de passe complexes et uniques, l'utilisation d'un gestionnaire de mots de passe est mise en œuvre au sein de notre collectivité.

## Protection des postes de travail

La sécurité physique de nos équipements est tout aussi importante que la sécurité logicielle. Il est essentiel de verrouiller systématiquement son poste de travail lors de toute absence, même brève, pour prévenir tout accès non autorisé.

Cette habitude simple mais efficace contribue grandement à la protection de nos données sensibles et à la préservation de la confidentialité de nos activités.

L'accès aux connecteurs USB représente une vulnérabilité potentielle, particulièrement dans les services recevant du public.

Pour atténuer ce risque, les postes de travail doivent être installés de manière à ce que le public n'ait pas d'accès direct aux ports USB. Cela peut être réalisé soit en positionnant de manière adaptée les boîtiers des ordinateurs, soit en les plaçant dans des caissons prévus à cet effet. Cette disposition physique des équipements constitue une barrière supplémentaire contre les accès non autorisés et les insertions potentielles de périphériques malveillants.

## Politique de sauvegarde

La sauvegarde régulière et fiable de nos données est cruciale pour assurer la continuité de nos activités et la protection de nos informations. Notre collectivité adopte la règle 3-2-1 pour les sauvegardes :

* Trois copies des données :
  + La copie originale
  + Deux sauvegardes distinctes
* Deux types de support différents :
  + Par exemple, un disque dur local et un stockage cloud sécurisé
* Une copie hors site :
  + Stockée dans un lieu géographiquement distant de nos locaux

Procédures de sauvegarde :

* Les sauvegardes automatiques sont effectuées quotidiennement pour les données critiques.
* Des sauvegardes complètes sont réalisées hebdomadairement.
* Les agents sont responsables de s'assurer que leurs données importantes sont bien incluses dans le périmètre de sauvegarde.

Sécurité des sauvegardes :

* Toutes les sauvegardes sont chiffrées.
* L'accès aux sauvegardes est strictement contrôlé et limité au personnel autorisé.

## Communication électronique et usage d'Internet

L'utilisation responsable d'Internet et de la messagerie électronique est essentielle à notre sécurité numérique.

Il est crucial d'être vigilant face aux pièces jointes et aux liens contenus dans les courriels, en s'abstenant d'ouvrir ou de cliquer sur des éléments suspects. Tout courriel suspect devra être signalé au référent cybersécurité pour avis.

Pour les communications internes, l'utilisation de notre plateforme de collaboration est à privilégier par rapport aux courriels, réduisant ainsi les risques liés aux échanges de courriels.

L'usage d'Internet dans le cadre professionnel doit se faire de manière responsable, en accord avec l'éthique et les valeurs de notre service public.

## Gestion des équipements et mises à jour

La maintenance régulière de nos équipements informatiques est cruciale pour maintenir un niveau de sécurité adéquat.

L'installation de logiciels doit être strictement encadrée et soumise à autorisation préalable.

Les mises à jour des systèmes d'exploitation et des logiciels antivirus doivent être effectuées régulièrement, constituant ainsi une première ligne de défense contre les menaces.

En cas de perte ou de vol d'un équipement, il est impératif de le signaler immédiatement pour permettre une réaction rapide et limiter les risques potentiels.

## Utilisation du Wifi

L'utilisation du Wifi dans nos locaux doit suivre des règles strictes pour garantir la sécurité de notre réseau.

Les bornes Wifi internes sont réservées exclusivement aux ordinateurs portables professionnels de la collectivité.

Pour les équipements personnels ou ceux de nos partenaires, seules les bornes Wifi internet non connectées à notre réseau local doivent être utilisées.

Cette séparation permet de maintenir un niveau élevé de sécurité tout en offrant une connectivité aux visiteurs.

## Gestion des périphériques amovibles

L'utilisation de périphériques amovibles, tels que les clés USB, présente des risques significatifs pour la sécurité de nos systèmes.

Pour minimiser ces risques, l'usage de clés USB est interdit. Les transferts de fichiers doivent se faire via les outils cloud sécurisés mis à disposition

Cette règle permet de réduire considérablement les risques d'infection par des logiciels malveillants et de perte de données sensibles.

## Politique de bureau propre

Une politique de bureau propre contribue à la sécurité physique de nos informations.

Les agents doivent s'assurer qu'aucun document sensible n'est laissé sur les bureaux en dehors des heures de travail.

Tous les documents papier contenant des informations confidentielles doivent être rangés dans des armoires verrouillées lorsqu'ils ne sont pas utilisés.

Cette pratique réduit les risques de fuite d'informations et renforce notre engagement envers la protection des données.

## Gestion des accès des prestataires externes

Les accès accordés aux prestataires externes doivent être strictement contrôlés et limités dans le temps.

Un processus formel d'octroi et de révocation des accès doit être mis en place, avec une révision régulière des droits accordés.

Cela permet de s'assurer que seuls les prestataires actuels ont accès à nos systèmes et uniquement dans la mesure nécessaire à l'accomplissement de leurs tâches.

## Procédure de départ des agents

Une procédure doit inclure la révocation immédiate de tous les accès, la récupération des équipements fournis, et la vérification qu'aucune donnée professionnelle n'est conservée sur des appareils personnels.

Cette procédure permet de prévenir les accès non autorisés post-emploi et de protéger les actifs informationnels de la collectivité.

Lorsqu'un agent bénéficie de congés avant une mobilité professionnelle ou un départ à la retraite, notamment grâce à l'utilisation d'un Compte Épargne Temps (CET) ou au cumul d'heures ou de congés, il est clairement défini dans notre politique que l'accès de l'agent est entièrement révoqué dès son dernier jour de travail effectif, sauf décision contraire justifiée par des besoins spécifiques du service et validée par la direction..

## Gestion des incidents

Face à l'éventualité d'un incident de cybersécurité, qu'il s'agisse d'une infection par un virus, d'un vol de données, ou d'une suspicion d'accès non autorisé, il est crucial d'agir rapidement et de manière organisée.

**Détection et signalement**

Tout utilisateur confronté à une situation suspecte doit immédiatement suivre les "Consignes en cas de cyberattaque" (voir Annexe 5) et informer le référent cybersécurité ou le directeur général des services.

Les signes d'une possible cyberattaque incluent :

* Ralentissement inhabituel des systèmes
* Fichiers chiffrés ou inaccessibles
* Messages d'erreur inhabituels
* Activités suspectes sur les comptes

**Premières actions**

* Débrancher immédiatement l'équipement suspect du réseau (câble réseau et Wi-Fi)
* Ne pas éteindre l'appareil pour préserver les preuves
* Ne plus utiliser l'équipement potentiellement compromis
* Prévenir les collègues d’une suspicion d'attaque en cours

**Mise en œuvre de la stratégie de réponse**

* Mettre en place une main courante pour relever les opérations
* Identifier si possible la source de l'attaque pour isoler les postes infectés
* Faire l'inventaire des ressources indisponibles
* Prévenir le CSIRT Régional compétent : 01.02.03.04.05
* Effectuer une déclaration sur <https://www.cybermalveillance.gouv.fr/>
* Informer le DPO en cas de violation de données personnelles

**En cas de perturbation importante**

* Mettre en place la cellule de crise restreinte prévue au PCS
* Préparer un communiqué de presse
* Contacter le prestataire informatique d'urgence
* Informer la Gendarmerie Nationale
* Utiliser le PCA pour identifier les conséquences prévisibles de la perturbation
* Débuter la mise en place des modes dégradés, tels que prévu au PCA.

**Communication**

* Interne : Informer les employés des mesures à prendre et de l'évolution de la situation
* Externe : Préparer une communication pour les usagers et les partenaires si nécessaire

**Restauration et retour à la normale**

* Vérifier que l'environnement n'a pas été compromis avant toute restauration
* Restaurer les services en débutant par ceux identifiés comme prioritaires au PCA

**Analyse post-incident : Après la résolution de l'incident, organiser une réunion d'analyse pour**

* Comprendre les causes de l'incident
* Évaluer l'efficacité de la réponse
* Identifier les améliorations nécessaires dans nos processus et systèmes

**Mise à jour du PCA**

À la suite de cette analyse, le Plan de Continuité d'Activité sera mis à jour pour intégrer les leçons apprises.

# Formation et sensibilisation

La formation et la sensibilisation constituent des éléments clés de notre stratégie de sécurité.

Des sessions de sensibilisation aux risques informatiques seront organisées pour l'ensemble des agents et des élus.

Ces sessions permettront d'actualiser les connaissances de chacun sur les menaces émergentes et les bonnes pratiques à adopter.

Elles seront également l'occasion d'échanger sur les expériences vécues et de renforcer notre culture collective de la sécurité.

# Conformité RGPD et protection des données personnelles

Notre collectivité s'engage à respecter le Règlement Général sur la Protection des Données (RGPD) dans toutes ses activités de traitement des données personnelles. Pour assurer cette conformité, nous avons nommé un Délégué à la Protection des Données (DPO) par arrêté du Maire. Pour cette mission uniquement, Le DPO est rattaché directement à la direction générale des services, garantissant ainsi son indépendance et son accès direct aux plus hauts niveaux de l'organisation.

Le rôle du DPO est crucial dans notre démarche de protection des données. Il est chargé de :

* Informer et conseiller la collectivité et ses employés sur leurs obligations en vertu du RGPD
* Surveiller la conformité au RGPD et aux politiques internes de protection des données
* Servir de point de contact pour les personnes concernées et l'autorité de contrôle (CNIL)
* Tenir à jour le registre des activités de traitement

Le registre des activités de traitement, tenu par le DPO, est un outil essentiel pour notre conformité. Il recense de manière simplifiée tous les traitements de données personnelles effectués par notre collectivité, permettant ainsi une vue d'ensemble de nos pratiques en matière de gestion des données. Ce registre nous aide à identifier les risques potentiels et à mettre en place les mesures de protection appropriées.

Tous les agents et élus doivent collaborer avec le DPO et lui signaler toute nouvelle activité de traitement de données ou toute modification d'un traitement existant. En cas de doute sur la conformité d'un traitement au RGPD, il est impératif de consulter le DPO avant sa mise en œuvre.

Les coordonnées du DPO en fonction sont disponibles auprès du secrétariat de la direction générale des services. N'hésitez pas à le contacter pour toute question relative à la protection des données personnelles.

# Sanctions

Le respect de cette politique de sécurité n’est pas facultatif, il est essentiel pour protéger notre commune et nos citoyens.

Bien que notre approche privilégie la pédagogie et la prévention, des manquements répétés ou graves à cette politique pourront entraîner des sanctions disciplinaires pour les agents ou la restriction temporaire ou permanente des accès aux systèmes d'information pour les élus.

# Annexes

1. **Plan de Continuité d'Activité (PCA)** Le tableau détaillé du Plan de Continuité d'Activité (PCA), mentionné dans la section Gestion des incidents, présente les procédures spécifiques à suivre pour chaque service municipal en cas de perturbation majeure de nos systèmes d'information, assurant ainsi la continuité en mode dégradé de nos services essentiels.
2. **Cartographie des équipements numériques** Ce document fournit un inventaire exhaustif de tous les équipements informatiques de la commune, incluant les ordinateurs, serveurs, équipements réseau, et autres dispositifs connectés. Cette cartographie est essentielle pour comprendre l'étendue de notre infrastructure numérique, identifier les points potentiellement vulnérables, et planifier efficacement les mises à jour et les mesures de sécurité.
3. **Liste des prestataires informatiques et de leurs sous-traitants** Cette annexe répertorie tous les prestataires externes impliqués dans la gestion, la maintenance ou le développement de nos systèmes d'information. Elle inclut les coordonnées de contact, la nature des services fournis, et les éventuels sous-traitants auxquels ces prestataires font appel. Ce document est crucial pour maintenir une vue d'ensemble de notre écosystème numérique et garantir que tous les acteurs impliqués respectent nos normes de sécurité.
4. **Fiche Bonnes pratiques pour les utilisateurs** Une fiche destinée à tous les utilisateurs, résumant les principales règles de sécurité à respecter au quotidien, comme la gestion des mots de passe, l'utilisation sécurisée de la messagerie, et les précautions à prendre face à un message suspect.
5. **Fiche Consignes en cas de cyberattaque** Cette fiche fournit des instructions claires et concises sur les actions immédiates à entreprendre en cas de suspicion de cyberattaque. Elle est conçue pour être facilement accessible et compréhensible par tous les agents, même en situation de stress.
6. **Fiche Premier canal d’attaque : le courriel** Cette fiche vise à sensibiliser aux risques liés aux courriels, l’un des principaux vecteurs d’attaques informatiques. Pour protéger les systèmes et les données sensibles, il est essentiel de reconnaître les signes d’une éventuelle compromission et d’adopter les bons réflexes.

Annexe 1 - Plan de Continuité d'Activité

Une image contenant texte, reçu, noir et blanc, nombre

Description générée automatiquement

Annexe 2 - Cartographie des équipements numériques

Une image contenant texte, capture d’écran, nombre, noir et blanc

Description générée automatiquement

Annexe 3- Liste des prestataires informatiques / sous-traitants

Une image contenant texte, capture d’écran, nombre, Police

Description générée automatiquement

Annexe 4- Fiche récapitulative sur les bonnes pratiques

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Annexe 5 - Fiche Consignes en cas de cyberattaque

Une image contenant texte, Appareils électroniques, capture d’écran, Page web

Description générée automatiquement

Annexe 6 – Fiche Premier canal d’attaque : le mail

Pour mieux protéger les systèmes informatiques et les informations importantes, il est crucial de faire attention aux signes qui pourraient montrer qu’une faille de sécurité s’est produite. Voici quelques exemples de situations qui demandent d’être vigilant.

**Courriels suspects provenant de contacts connus**

Réception d’un courriel inhabituel contenant des liens ou des pièces jointes suspects, même s’il semble provenir d’un contact connu ou d’une adresse légèrement modifiée.

Une attention particulière doit être portée aux adresses de courriel qui imitent celles de collègues ou de partenaires, mais qui présentent de légères variations.

Une image contenant texte, Appareils électroniques, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

**Demandes urgentes ou inhabituelles**

Courriels demandant une action immédiate, comme un virement bancaire, une confirmation de données sensibles ou une réponse rapide sous pression.

Ces messages peuvent contenir des menaces implicites ou être rédigés dans un style ou avec une orthographe inhabituelle.

**Courriels concernant un partage de fichiers avec demande d’identifiants**

Messages prétendant provenir de services de partage de fichiers (exemple : OneDrive, Google Drive) redirigeant vers une page de connexion pour saisir des identifiants.

Ces tentatives d’hameçonnage visent à voler des informations d’authentification.

Une image contenant texte, Appareils électroniques, capture d’écran, Page web

Le contenu généré par l’IA peut être incorrect.

Une image contenant texte, capture d’écran, Page web, Site web

Le contenu généré par l’IA peut être incorrect.

**Alertes d’activités suspectes**

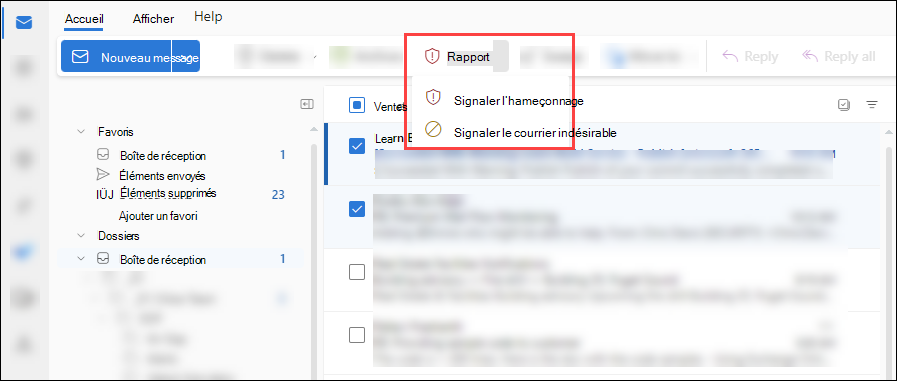
Notifications de connexions inhabituelles, changements de mot de passe non sollicités ou autres alertes émises par les systèmes de sécurité.

Ces alertes peuvent indiquer qu’un tiers tente d’accéder à un compte ou aux systèmes.

**Procédure de signalement d’un courriel suspect**

En cas de réception d’un courriel frauduleux, celui-ci doit être sélectionné, puis l’option Signaler doit être cliquée en choisissant Signaler l’hameçonnage.

Cette action permet d’alerter les services concernés et de renforcer la sécurité globale en bloquant les menaces potentielles.



En cas de comportement suspect ou de doute, il est impératif de le signaler immédiatement au service informatique. Une analyse approfondie sera réalisée, et des mesures correctives pourront être mises en place pour limiter les risques et protéger les systèmes et données.