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.

Dernière mise à jour le xxxxxxxxxx

1. 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.

2. 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.

3. Règles de base

3.1 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.

3.2 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.

3.3 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.

3.4 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.

3.5 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.

3.6 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.

3.7 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.

3.8 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.

3.9 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.

3.10 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..

3.11 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.

4. 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.

5. 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.

6. 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.

7. 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

Service	Mission	Tâche	Support utilisé	Hébergement	Délai de mise en place du mode dégradé	Tâches en mode dégradé	Supports en mode dégradé	A préparer en amont
État civil	Enregistrement des naissances	Saisie des déclarations	Logiciel GRC	Externalisé (Berger-Levrault)	Immédiat	Remplissage manuel des actes	Registres papier pré-imprimés	Imprimer et stocker des registres vierges
Urbanisme	Instruction droit des sols	Consultation cadastre, PLU	XMap cartographie	Externalisé (Sirap)	3 mois	Utilisation de cadastre.gouv.fr	Autre ordinateur	
Finances	Mandatement	Émission de mandats	EGF	Externalisé (Berger-Levrault)	1 mois	Élaboration manuelle des mandats	Formulaires papier	Stocker des formulaires vierges
RH	Gestion des congés	Validation des demandes	E-congés	Interne (Hôtel de Ville)	Immédiat	Utilisation de formulaires papier	Formulaires de demande	Imprimer des formulaires de congés
Communication	Gestion du site internet	Mise à jour du contenu	Wordpress	Externalisé (OVH)	7 jours	Publication sur les réseaux sociaux	Smartphone de service	Préparer des modèles de posts
Police municipale	Verbalisation	Saisie des infractions	Logiciel PVe	Externalisé (ANTAI)	Immédiat	Utilisation de carnets à souche	Carnets de verbalisation	Stocker des carnets de verbalisations
Services techniques	Gestion des interventions	Planification des travaux	OpenGST	Externalisé (Arpège)	7 jours	Planning manuel sur tableau	Tableau blanc, marqueurs	Préparer un modèle de planning
CCAS	Aide sociale	Instruction des demandes	Logiciel Elisaar	Externalisé (Elisaar)	15 jours	Formulaires papier	Dossiers papier	Imprimer des formulaires de demande
Accueil	Gestion du standard	Réception et transfert d'appels	Standard téléphonique IP	Externalisé (Orange)	Immédiat	Utilisation de téléphones portables	Téléphones portables de secours	Tenir à jour une liste des numéros importants
Marchés publics	Publication des appels d'offres	Mise en ligne des DCE	Plateforme de dématérialisation	Externalisé (AWS)	7 jours	Envoi par courrier sur demande	Photocopieuse, papier	Préparer des modèles de DCE imprimables
Scolaire	Inscriptions cantines	Gestion des inscriptions	Logiciel Abelium	Externalisé (Abelium)	1 mois	Fiches d'inscription papier	Classeurs, fiches papier	Imprimer des fiches d'inscription
Culture	Billetterie spectacles	Vente et réservation	Logiciel Elisath	Externalisé (Elisath)	Immédiat	Billetterie manuelle	Carnets à souches	Stocker des carnets à souches
Sport	Réservation des équipements	Gestion du planning	OpenGST	Externalisé (Arpège)	7 jours	Planning papier	Tableau d'affichage	Préparer un modèle de planning hebdomadaire
Élections	Tenue des listes électorales	Inscriptions, radiations	REU	Externalisé (INSEE)	1 mois	Registre papier	Cahier d'émargement	Imprimer régulièrement la liste électorale
Juridique	Suivi des contentieux	Gestion des dossiers	SharePoint	Externalisé (Microsoft)	15 jours	Dossiers papier	Armoires sécurisées	Imprimer régulièrement un état des affaires en cours
Cimetière	Gestion des concessions	Attribution des emplacements	Logiciel Gescime	Externalisé (Gescime)	1 mois	Registre papier	Registre, plan papier	Imprimer régulièrement le plan du cimetière
Bibliothèque	Prêt de documents	Enregistrement des prêts	Logiciel Orphée	Externalisé (C3RB)	Immédiat	Fiches de prêt manuelles	Fiches cartonnées	Préparer des fiches de prêt
Petite enfance	Inscriptions crèche	Gestion des dossiers	Logiciel Abelium	Externalisé (Abelium)	15 jours	Dossiers papier	Formulaires, classeurs	Imprimer des dossiers d'inscription vierges
Patrimoine	Inventaire des biens	Mise à jour de l'inventaire	Logiciel Astech	Externalisé (Astech)	3 mois	Tableur Excel	PC portable de secours	Exporter régulièrement l'inventaire en Excel
Archives	Consultation des documents	Recherche et mise à disposition	Logiciel Mnesys	Externalisé (Naxoned)	7 jours	Inventaire papier	Registres d'inventaire	Imprimer annuellement l'inventaire des archives
Environnement	Suivi des espaces verts	Planification des interventions	OpenGST	Externalisé (Arpège)	15 jours	Planning mural	Tableau blanc magnétique	Préparer un modèle de planning saisonnier
Associations	Gestion des subventions	Instruction des demandes	Excel	Externalisé (Microsoft)	1 mois	Dossiers papier	Formulaires, classeurs	Imprimer des formulaires de demande de subvention
DGS	Suivi des projets	Tableaux de bord	Microsoft Project	Externalisé (Microsoft)	7 jours	Tableaux de suivi papier	Panneau d'affichage	Imprimer mensuellement l'état d'avancement des projets
État civil	Célébration des mariages	Planification des cérémonies	Outlook	Externalisé (Microsoft)	Immédiat	Agenda papier	Cahier de rendez-vous	Imprimer hebdomadairement le planning des mariages
Urbanisme	Délivrance des permis	Instruction des demandes	Logiciel Cart@DS	Externalisé (ATREAL)	1 mois	Dossiers papier	Formulaires CERFA, classeurs	Stocker des formulaires CERFA vierges
Finances	Gestion de la dette	Suivi des emprunts	Logiciel Finance Active	Externalisé (Finance Active)	3 mois	Tableau Excel	PC portable de secours	Exporter trimestriellement l'état de la dette
RH	Gestion de la paie	Édition des bulletins	CIRIL RH	Externalisé (CIRIL Group)	15 jours	Calculs manuels	Tableur Excel, calculatrice	Préparer un modèle de calcul de paie simplifié
Communication	Gestion des panneaux d'affichage	Diffusion des messages	Logiciel LumiPlan	Externalisé (Lumiplan)	7 jours	Affichage manuel	Panneaux d'affichage classiques	Stocker des affiches vierges
Police municipale	Gestion des objets trouvés	Enregistrement et restitution	Excel	Externalisé (Microsoft)	Immédiat	Registre papier	Cahier, stylos	Préparer un modèle de fiche objet trouvé
Services techniques	Gestion du parc automobile	Suivi des entretiens	Logiciel GMAO	Interne (Hôtel de Ville)	1 mois	Fiches de suivi par véhicule	Classeur, fiches papier	Imprimer des fiches de suivi pour chaque véhicule
CCAS	Portage des repas	Planification des tournées	Logiciel Domatel	Externalisé (Implicit)	7 jours	Planning papier	Tableau blanc, marqueurs	Préparer un modèle de planning hebdomadaire
Accueil	Gestion du courrier	Enregistrement arrivée/départ	Logiciel DOTELEC	Externalisé (DIGITECH)	Immédiat	Cahier d'enregistrement	Cahier, tampon dateur	Préparer un modèle de cahier d'enregistrement
Marchés publics	Analyse des offres	Notation des candidats	Excel	Externalisé (Microsoft)	15 jours	Grilles d'analyse papier	Calculatrice, stylos	Imprimer des grilles d'analyse vierges
Scolaire	Gestion des transports scolaires	Inscription aux circuits	Logiciel Pégase	Externalisé (OIFI)	1 mois	Listes d'inscription papier	Classeurs, fiches	Imprimer des fiches d'inscription par circuit
Culture	Gestion de la médiathèque	Catalogage des ouvrages	Logiciel Orphée	Externalisé (C3RB)	1 mois	Fiches descriptives papier	Fiches cartonnées, classeurs	Préparer des modèles de fiches de catalogage
Sport	Gestion des associations sportives	Suivi des créneaux	Excel	Externalisé (Microsoft)	15 jours	Planning mural	Tableau blanc magnétique	Préparer un planning type par équipement
Élections	Organisation des scrutins	Composition des bureaux de vote	Excel	Externalisé (Microsoft)	7 jours	Tableau papier	Panneau d'affichage	Imprimer la liste des électeurs volontaires
DGS	Gestion des arrêtés municipaux	Rédaction et publication	Logiciel AirsDelib	Externalisé (Digitech)	15 jours	Rédaction manuelle	Modèles papier, classeurs	Stocker des modèles d'arrêtés types
Cimetière	Gestion des exhumations	Planification des opérations	Excel	Externalisé (Microsoft)	1 mois	Agenda papier	Cahier de rendez-vous	Préparer un modèle de fiche d'exhumation
Bibliothèque	Gestion des animations	Planification des événements	Outlook	Externalisé (Microsoft)	15 jours	Agenda papier	Cahier de bord	Imprimer mensuellement le programme des animations

Annexe 2 - Cartographie des équipements numériques

Type d'équipement	Marque/Modèle	Localisation	Utilisateur principal	Date d'achat	Connecté	Descriptif	Niveau de sensibilité	Numéro de série
Ordinateur fixe	Dell Optiplex 3080	Bureau du maire	Maire	15/03/2022	Oui	PC principal du maire	Très élevé	DELL78901234
Ordinateur portable	Lenovo ThinkPad T14	Service technique	Chef de service	10/01/2023	Oui	Utilisé pour la gestion des projets techniques	Élevé	LEN20230110T14
Serveur	HP ProLiant DL360	Local technique	N/A	05/06/2021	Oui	Serveur principal, héberge les données critiques	Très élevé	HPSERV210605
Imprimante réseau	HP LaserJet Pro M404dn	Accueil	Tous	22/11/2022	Oui	Imprimante multifonction pour documents généraux	Moyen	HPLAS221122DN
Ordinateur fixe	Dell Optiplex 3070	Service RH	Responsable RH	20/04/2021	Oui	Gestion des dossiers du personnel	Très élevé	DELL71234567
Tablette	iPad Air 2022	Service communication	Chargé de com	03/07/2023	Wi-Fi	Utilisée pour les réseaux sociaux et la communication	Moyen	IPAD230703A1
Ordinateur portable	HP EliteBook 840	Direction générale	DGS	12/12/2022	Oui	PC principal du DGS, accès aux données stratégiques	Très élevé	HPEB221212840
Switch réseau	Cisco Catalyst 2960	Local technique	N/A	15/08/2021	Oui	Switch principal pour le réseau local	Élevé	CISC21081560
NAS	Synology DS220+	Local technique	N/A	30/09/2022	Oui	Stockage de fichiers et sauvegardes locales	Élevé	SYN220930DS2
Ordinateur fixe	Dell Optiplex 3060	Service urbanisme	Agent urbanisme	05/05/2020	Oui	Gestion des permis de construire et cadastre	Élevé	DELL60200505
Ordinateur portable	Lenovo ThinkPad X1 Carbon	Service finances	Responsable finances	18/02/2023	Oui	Gestion du budget et comptabilité	Très élevé	LENX1230218C
Scanner	Epson WorkForce DS-870	Service état civil	Agent état civil	07/11/2022	Oui	Numérisation des actes et documents officiels	Élevé	EPSC221107DS
Ordinateur fixe	HP ProDesk 400 G6	Accueil	Agent d'accueil	10/06/2021	Oui	Point d'accueil principal	Moyen	HPPD21061OG6
Firewall	Fortinet FortiGate 60F	Local technique	N/A	22/03/2022	Oui	Protection périmétrique du réseau	Très élevé	FORT22032260
Ordinateur portable	Dell Latitude 5420	Service jeunesse	Animateur	14/09/2022	Wi-Fi	Gestion des activités jeunesse et planification	Moyen	DELL22091454
Téléphone IP	Yealink T53W	Tous bureaux	Tous	01/04/2021	Oui	Téléphonie VoIP	Faible	YEAL21040153
Vidéoprojecteur	Epson EB-2250U	Salle de réunion	N/A	25/10/2021	Wi-Fi	Présentations et réunions	Faible	EPSN21102522
Ordinateur fixe	HP EliteDesk 800 G6	Service marchés publics	Juriste	03/08/2022	Oui	Gestion des appels d'offres et contrats	Élevé	HPED220803G6
Borne Wi-Fi	Ubiquiti UniFi AP AC Pro	Étage administration	N/A	11/01/2023	Oui	Couverture Wi-Fi pour les bureaux	Moyen	UBIQ23011101
Ordinateur portable	Microsoft Surface Laptop 4	Élu adjoint	Adjoint au maire	09/05/2023	Wi-Fi	Utilisé pour les déplacements et réunions	Élevé	MSFT23050904

Annexe 3- Liste des prestataires informatiques / sous-traitants

Nom du prestataire	Service fourni	Coordonnées	Sous-traitant(s)	Accès aux systèmes
InfoTech Solutions	Maintenance du parc informatique	contact@infotech.fr, 01 23 45 67 89	Aucun	Accès administrateur sur les postes de travail
CloudSafe	Hébergement et sauvegarde	support@cloudsafe.com, 09 87 65 43 21	DataCenter Pro (hébergement physique)	Accès limité aux serveurs de sauvegarde
CyberGuard	Audit de sécurité annuel	securite@cyberguard.fr, 06 12 34 56 78	Aucun	Accès temporaire pendant les audits
LogiMairie	Logiciel de gestion communale	support@logimairie.fr, 04 56 78 90 12	Aucun	Accès à distance pour maintenance
RéseauLocal	Installation et maintenance réseau	contact@reseaulocal.fr, 05 67 89 01 23	Aucun	Accès administrateur sur les équipements réseau
WebCommune	Hébergement et maintenance du site web	info@webcommune.com, 02 34 56 78 90	CloudHost (hébergement)	Accès FTP et base de données
TelePro	Téléphonie IP	support@telepro.fr, 03 45 67 89 01	VoIPConnect (trunk SIP)	Accès au central téléphonique virtuel
PrintService	Maintenance des imprimantes	service@printservice.fr, 04 32 10 98 76	Aucun	Accès limité aux imprimantes
ArchivSafe	Archivage électronique	contact@archivsafe.com, 05 43 21 09 87	SecureStore (stockage longue durée)	Accès limité à la plateforme d'archivage
FormaMairie	Formation informatique	formation@formamairie.fr, 06 54 32 10 98	Aucun	Aucun accès direct
AssistMairie	Assistance utilisateurs	support@assistmairie.com, 07 65 43 21 09	Aucun	Accès à distance sur autorisation
SécuritéPlus	Antivirus et pare-feu	info@securiteplus.fr, 08 76 54 32 10	VirusShield (mise à jour des définitions)	Accès à la console d'administration
GéoCommune	SIG et cartographie	contact@geocommune.fr, 09 87 65 43 21	MapData (données cartographiques)	Accès à la plateforme SIG
VisioConf	Solution de visioconférence	support@visioconf.com, 01 12 23 34 45	Aucun	Accès administrateur à la plateforme
DématAct	Dématérialisation des actes	contact@dematact.fr, 02 23 34 45 56	LegalTech (signature électronique)	Accès à la plateforme de dématérialisation
ElecMairie	Gestion des listes électorales	support@elecmairie.com, 03 34 45 56 67	Aucun	Accès au logiciel de gestion électorale
BudgetPro	Logiciel de comptabilité publique	compta@budgetpro.fr, 04 45 56 67 78	Aucun	Accès à distance pour support
CivilNet	Logiciel d'état civil	info@civilnet.com, 05 56 67 78 89	SecurePrint (impression sécurisée)	Accès au logiciel d'état civil
UrbaWeb	Gestion de l'urbanisme en ligne	contact@urbaweb.fr, 06 67 78 89 90	Aucun	Accès à la plateforme d'urbanisme
PayePublic	Logiciel de paie	support@payepublic.com, 07 78 89 90 01	LegalUpdate (mises à jour réglementaires)	Accès au logiciel de paie

Annexe 4- Fiche récapitulative sur les bonnes pratiques

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

VILLE D'ARCADIE

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

LES BONNES PRATIQUES

1. Ne **pas télécharger**, ni utiliser de logiciels, d'applications et de vidéos piratés ou **d'origine douteuse** qui peuvent souvent contenir un virus.
2. Ne **jamais désactiver votre antivirus** à la demande d'un logiciel.
3. Face à un **message suspect** (inattendu, alarmiste, aguicheur…), **ne pas ouvrir les pièces jointes** ou cliquer sur les liens.
4. **Mettre régulièrement à jour** vos appareils, logiciels et applications.
5. **Utiliser des mots de passe forts** qui ne disent rien sur vous et différents pour chaque accès afin d'éviter des piratages en cascade.
6. Deux sécurités valent mieux qu'une : **activer la double authentification** lorsque cela vous est proposé.
7. **Ne pas stocker vos mots de passe de manière non sécurisée** : post-it, fichiers textes, messages brouillons, notes sur votre smartphone…
8. Utiliser un **gestionnaire de mots de passe** ou un trousseau d'accès sécurisés, stockés de préférence en local, pour conserver vos mots de passe en sécurité. Vous n'aurez ainsi à retenir qu'un mot de passe pour accéder à l'ensemble de vos comptes.
9. Ne **jamais sauvegarder vos mots de passe dans le navigateur** d'un ordinateur partagé.
10. **Se déconnecter systématiquement de votre compte** après utilisation, pour éviter que quelqu'un puisse y accéder après vous.

RETROUVEZ TOUTES NOS PUBLICATIONS SUR :
www.cybermalveillance.gouv.fr

Version 1.0

Annexe 5 - Fiche Consignes en cas de cyberattaque

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

VILLE D'ARCADIE

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

CONSIGNES EN CAS DE CYBERATTAQUE

1 DÉBRANCHEZ LA MACHINE D'INTERNET OU DU RÉSEAU INFORMATIQUE

Débranchez le câble réseau et désactivez la connexion Wi-Fi ou les connexions de données pour les appareils mobiles.

2 N'ÉTEIGNEZ PAS L'APPAREIL

Certains éléments de preuve contenus dans la mémoire de l'équipement et nécessaires aux investigations seront effacés s'il est éteint.

3 ALERTEZ AU PLUS VITE VOTRE SUPPORT INFORMATIQUE

Votre support pourra prendre les mesures nécessaires pour contenir, voire réduire, les conséquences de la cyberattaque.

4 N'UTILISEZ PLUS L'ÉQUIPEMENT POTENTIELLEMENT COMPROMIS

Ne touchez plus à l'appareil pour éviter de supprimer des traces de l'attaque utiles pour les investigations à venir.

5 PRÉVENEZ VOS COLLÈGUES DE L'ATTAQUE EN COURS

Une mauvaise manipulation de la part d'un autre collaborateur pourrait aggraver la situation.

Pour vous informer sur les bonnes pratiques
et les principales menaces en matière de cybersécurité
rendez-vous sur :
www.cybermalveillance.gouv.fr

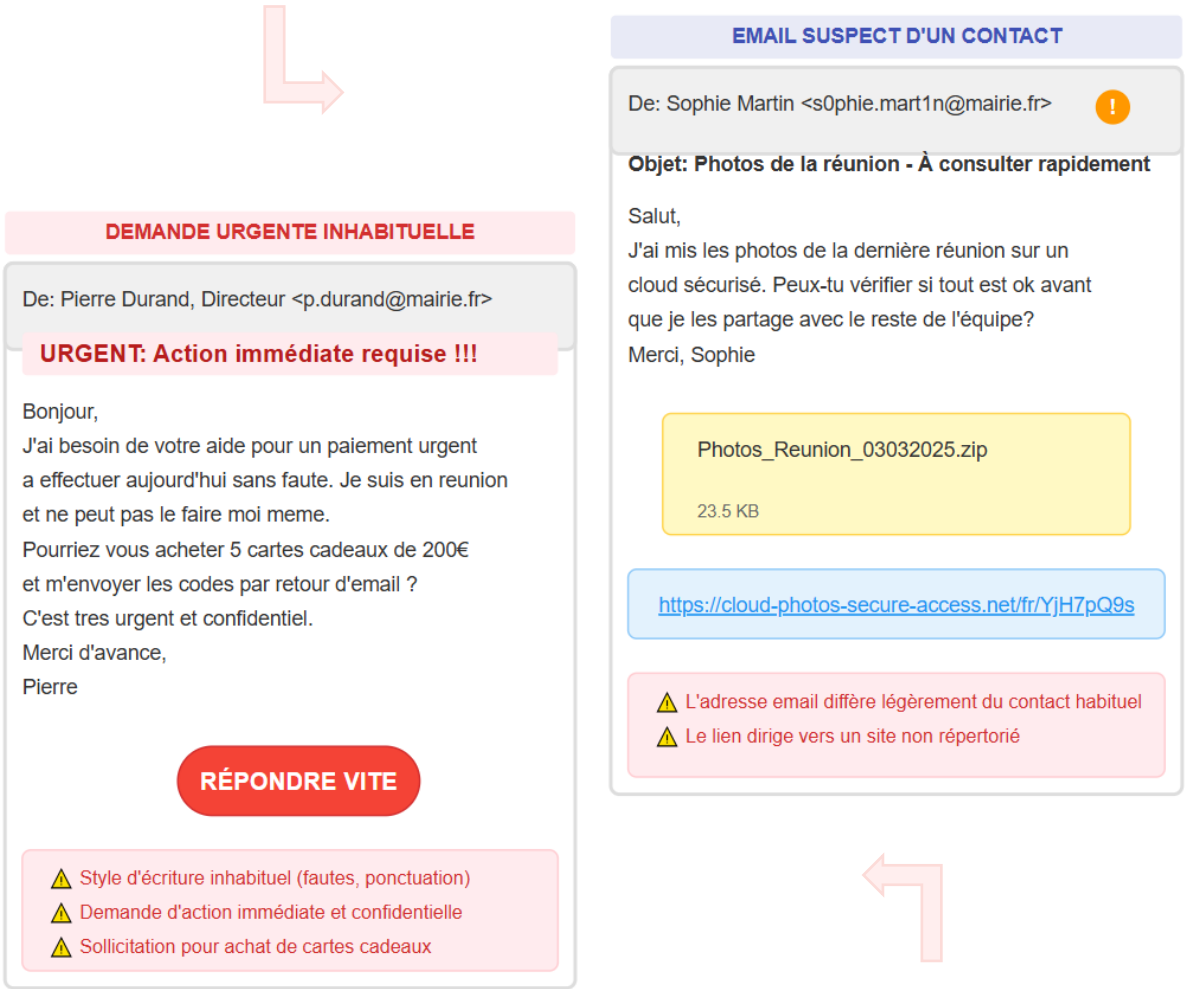
Annexe 6 – Fiche Premier canal d'attaque : le mail

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.



Demandes urgentes ou inhabituelles

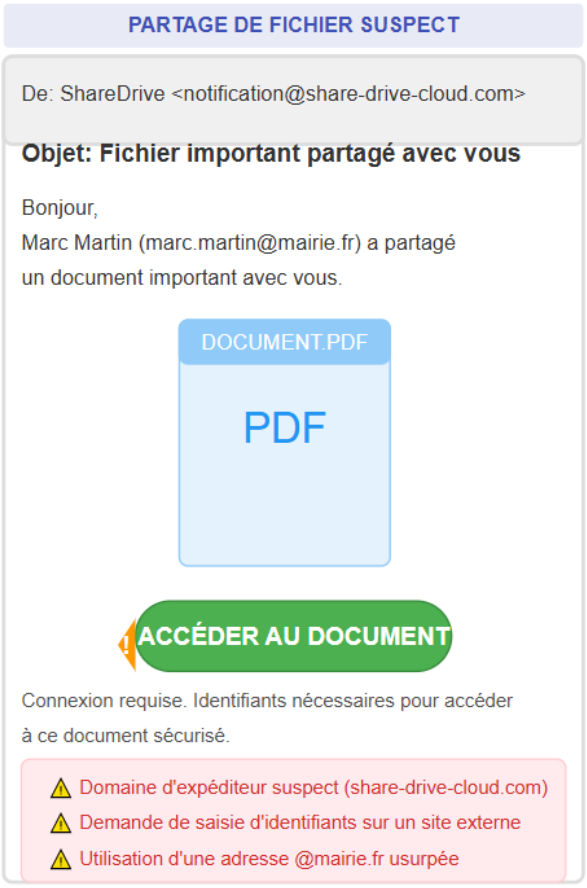
Courriels demandant une action immédiate, comme un virement bancaire, une confirmation de données sensibles ou une réponse rapide sous pression.

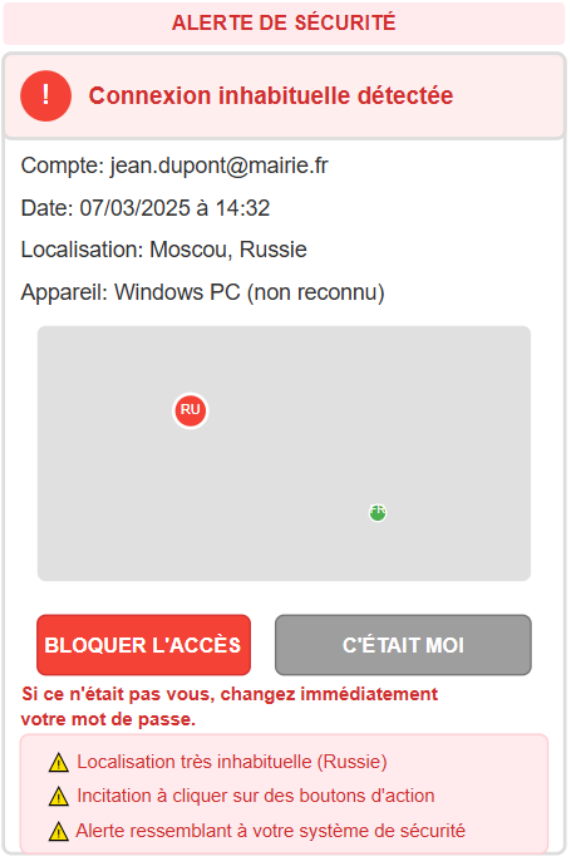
Ces messages peuvent contenir des menaces implicites ou être rédigés dans un style ou avec une orthographe inhabituelle.

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.





Alertes d'activités suspectes

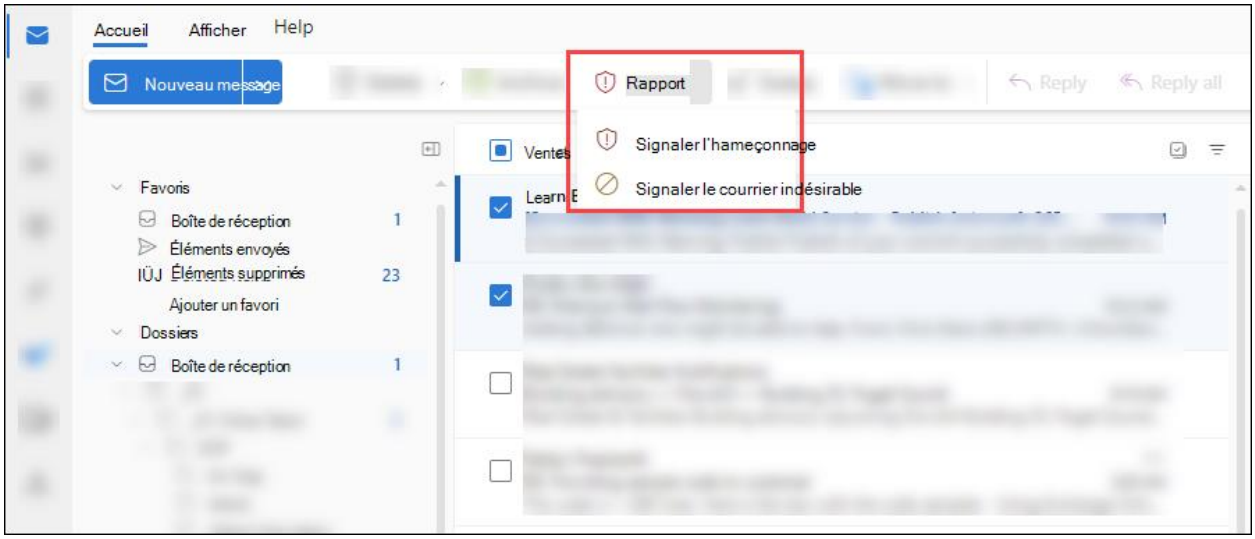
Notifications de connexions inhabituelles, changements de mot de passe non sollicités ou autres alertes émises par les systèmes de sécurité.

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.