Note interne relative à la modernisation de nos systèmes d'information

A l'attention des élus et des agents

Introduction et objectifs

Dans un contexte de transformation numérique accélérée et face à l'augmentation des cybermenaces, notre collectivité s'engage résolument dans la modernisation et la sécurisation de nos systèmes d'information. Cette note vise à vous informer des changements importants dans nos pratiques numériques et à vous présenter notre feuille de route pour les mois à venir.

Le conseil municipal a récemment adopté notre Politique de Sécurité des Systèmes d'Information (PSSI) simplifiée, marquant ainsi notre engagement formel dans cette démarche. Cette politique, annexée à la présente note, définit le cadre de nos actions en matière de cybersécurité.

La PSSI simplifiée : notre bouclier numérique

La PSSI simplifiée est un document stratégique qui définit les règles et pratiques essentielles pour protéger nos systèmes d'information et les données de nos citoyens. Élaborée de manière collaborative, elle s'adapte à notre réalité de collectivité territoriale.

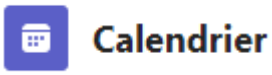
Grands principes de la PSSI :

1. Protection des données personnelles et sensibles
2. Gestion des accès et des identités
3. Sécurisation des infrastructures
4. Formation et sensibilisation des utilisateurs
5. Gestion des incidents de sécurité

La PSSI simplifiée est annexée à cette note.

Évolution de nos pratiques numériques

Utilisation du calendrier partagé



L'utilisation du calendrier partagé dans notre collectivité vise à améliorer la **coordination** des réunions, des projets et des tâches au sein des équipes. Cette fonctionnalité facilite la planification, réduit les conflits d'horaires et améliore la visibilité sur les disponibilités de chacun, contribuant ainsi à une meilleure organisation du temps de travail.

Tous les utilisateurs disposent d'un calendrier professionnel qu'ils doivent consulter régulièrement car des réunions peuvent y être ajoutées à tout moment. Par défaut, tous les utilisateurs peuvent consulter le calendrier des autres agents de la collectivité, ce qui permet de planifier les réunions en fonction des disponibilités de chacun. L'objet des rendez-vous n'est pas visible, mais la disponibilité (disponible/non disponible) apparaît. Chaque utilisateur est libre de partager le détail de son calendrier avec qui il le souhaite, comme son binôme, son secrétariat ou sa hiérarchie.

Les partenaires ou prestataires extérieurs peuvent également être invités aux réunions de notre collectivité via leur adresse e-mail. **Toutes les réunions de la collectivité sont ainsi convoquées exclusivement par le biais des calendriers partagés**, y compris avec des intervenants extérieurs.

Conformément à nos engagements de réduction des documents papiers, confirmés par la loi n° 2019-1461 du 27 décembre 2019 relative à l'engagement dans la vie locale et à la proximité de l'action publique, les convocations « papiers » sont totalement supprimées.

Gestion des fichiers et abandon des supports physiques

Pour renforcer notre sécurité et faciliter la collaboration :

- L'utilisation des clés USB est désormais interdite en raison des risques de propagation de virus.
- Le serveur de fichier historique (#commun) a été supprimé et ne doit pas être recréé.
- Les fichiers doivent être stockés dans OneDrive (pour l'usage individuel) ou dans les équipes/canaux Teams (pour l'usage collectif).

Fichiers à usage individuel

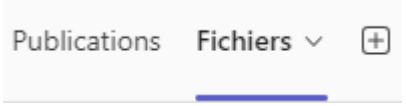
Chaque utilisateur dispose d'un accès à un **dossier OneDrive individuel**. Ce dernier est sécurisé, sauvegardé et accessible depuis n'importe quel ordinateur où l'utilisateur se connecte. Il peut ainsi téléverser tout fichier de la même manière qu'il le ferait en copiant des fichiers sur une clé USB pour les utiliser sur un autre ordinateur. Pour simplifier davantage la gestion des fichiers, chaque utilisateur peut apprendre à synchroniser son dossier « Documents » avec son OneDrive individuel. De plus, contrairement à des solutions

fermement déconseillées telles que WeTransfer ou Grosfichiers, le partage de fichiers OneDrive offre un niveau de sécurité supplémentaire, permettant un échange sécurisé de données sensibles tout en facilitant la collaboration.

Fichiers à usage collectif

En tant qu'agents accomplissant des missions de service public, il est essentiel d'assurer une continuité de fonctionnement. C'est pourquoi tous les documents de travail, la documentation, les fichiers de suivi et les éléments financiers doivent être partagés avec les collègues ou la hiérarchie. Ainsi, en cas d'absence ou de départ d'un collaborateur, la continuité des activités est assurée. De plus, certains documents exploités aujourd'hui pourraient être nécessaires dans plusieurs années, probablement par d'autres personnes, pour mener à bien la clôture ou la poursuite d'un dossier. Il est donc important de conserver et de stocker ces documents de manière sécurisée et organisée.

Pour ce faire, tous les fichiers relatifs à un sujet, qu'ils soient des documents finalisés ou des documents de travail en cours de rédaction, doivent **être stockés dans le canal de l'équipe qui concerne ce sujet**. Dans l'onglet "Fichiers", il est possible de ranger les fichiers par répertoires, comme on le ferait sur un disque dur ou un serveur de fichiers.



Cette méthode de gestion des fichiers à usage collectif permet de centraliser les informations, de faciliter la collaboration et de garantir la sécurité et la pérennité des données.

Communication interne et externe

L'arrivée de Teams comme nouvel outil de communication peut être déstabilisante pour certains, mais il est important d'établir des règles d'utilisation communes pour optimiser l'efficacité de nos échanges et renforcer notre sécurité.

Utilisation de la messagerie électronique

- La boîte mail professionnelle reste l'outil essentiel de communication avec les interlocuteurs extérieurs à notre collectivité.
- Chaque utilisateur de la plateforme Microsoft 365 doit utiliser exclusivement l'adresse mail professionnelle qui lui est attribuée.
- L'ouverture d'une boîte mail personnelle sur un outil professionnel, connecté au réseau interne, est strictement interdite et considérée comme une faille de sécurité potentielle.

Utilisation de Teams

- Pour la communication interne, Teams devient l'outil exclusif à utiliser.
- Les échanges de mails entre deux interlocuteurs internes doivent être évités au profit de l'utilisation de Teams.
- Cette approche permet de réduire les risques liés aux cyberattaques en utilisant des outils sécurisés pour nos communications internes.

Gestion des notifications

- Nous encourageons une gestion raisonnée des notifications pour préserver la concentration de chacun.
- Il est important de se rappeler que ni le mail ni le message Teams ne sont des outils de communication à utiliser en cas d'urgence. Dans de tels cas, privilégiez le SMS ou l'appel téléphonique.
- Aucun utilisateur n'est tenu de répondre immédiatement aux messages. Nous vous encourageons à désactiver les notifications instantanées qui ne sont pas nécessaires.
- Une lecture quotidienne des messages est généralement suffisante pour maintenir une communication efficace.

En adoptant ces pratiques, nous visons à améliorer notre efficacité collective tout en renforçant notre sécurité informatique. N'hésitez pas à personnaliser les paramètres de notification de vos outils de communication pour trouver le juste équilibre entre réactivité et concentration.

Utilisation du Wi-Fi dans nos locaux

Deux types de bornes Wi-Fi sont disponibles :

1. Bornes internes connectées à notre réseau local : réservées exclusivement aux ordinateurs portables professionnels de la collectivité. Aucun téléphone portable personnel ne doit être connecté sur ces bornes. L'identifiant réseau de ces bornes est XXXX.

2. Bornes Wi-Fi internet non connectées à notre réseau local : destinées aux équipements des partenaires ou élus pour un accès internet ponctuel. L'identifiant réseau de ces bornes est XXXX.

Gestion des données sensibles et conformité RGPD

La protection des données personnelles et sensibles est au cœur de nos préoccupations. Nous nous engageons à respecter scrupuleusement le Règlement Général sur la Protection des Données (RGPD).

Principes clés :

- Minimisation des données : nous ne collectons et ne traitons que les données strictement nécessaires à nos missions.
- Limitation de la durée de conservation : les données sont conservées uniquement pour la durée nécessaire à la finalité du traitement.
- Sécurisation des accès : seules les personnes habilitées ont accès aux données sensibles.
- Transparence : nous informons clairement les citoyens sur l'utilisation de leurs données.

Rôle du Délégué à la Protection des Données (DPO)

Notre DPO, Delphine Arcadienne, veille au respect de ces principes. Elle est votre interlocutrice privilégiée pour toute question relative à la protection des données. N'hésitez pas à la solliciter pour :

- Des conseils sur le traitement des données personnelles
- L'évaluation de la conformité RGPD de vos projets
- La gestion des demandes d'exercice des droits des personnes concernées

Stockage sécurisé des données sensibles

- Les données sensibles doivent être stockées dans Teams, dans des canaux privés ou avec des permissions spécifiques.
- L'utilisation de OneDrive pour les données sensibles est autorisée uniquement pour un usage temporaire et individuel.
- Le versement direct de fichiers sensibles dans SharePoint est strictement déconseillé.

Le Plan de Continuité d'Activité (PCA) : notre garantie de résilience

Le PCA est un outil essentiel pour assurer la continuité de nos services en cas de crise majeure, y compris les cyberattaques. Sa conception est terminée, il devient une annexe de notre PSSI, vous le trouverez joint, il implique tous les services de notre collectivité.

Le Plan de Continuité d'Activité (PCA) repose sur une approche méthodique visant à garantir que nos missions essentielles puissent se poursuivre même en cas de perturbations majeures. Pour ce faire, nous avons établi un inventaire détaillé de toutes les missions et tâches effectuées via nos outils numériques. Chaque tâche a ensuite été évaluée en termes de priorité, en déterminant le délai de rétablissement nécessaire pour assurer sa continuité. Cela nous permet de concentrer nos efforts sur les activités les plus critiques en cas de crise.

Une fois les tâches prioritaires identifiées, nous avons conçu des solutions alternatives pour les réaliser en mode dégradé. Cela implique de réfléchir à des méthodes de travail qui ne dépendent pas des technologies numériques. Par exemple, nous pouvons développer des formulaires papier, des plans manuels, et des registres physiques pour assurer la continuité des opérations essentielles.

Anticiper le mode dégradé ne se limite pas à la simple préparation de ces outils alternatifs. Il s'agit également de former les agents à leur utilisation, de tester régulièrement ces méthodes pour s'assurer de leur efficacité, et de maintenir à jour l'ensemble des ressources nécessaires. En adoptant cette approche proactive, nous nous assurons que, même en cas de défaillance technologique, notre collectivité peut continuer à fonctionner de manière cohérente et organisée, minimisant ainsi l'impact sur le service rendu aux usagers.

Le PCA sera intégré à notre Plan Communal de Sauvegarde (PCS) pour une approche globale de la gestion des risques.

Notre feuille de route pour renforcer la cybersécurité

Formation et sensibilisation

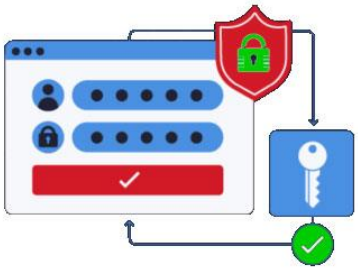
Un programme de formation sera mis en place pour améliorer les compétences numériques de tous les acteurs de notre collectivité. Ces formations couvriront :

- L'utilisation sécurisée des outils numériques
- La reconnaissance des menaces cyber (phishing, ransomware, etc.)
- Les bonnes pratiques de protection des données personnelles

Renforcement de la sécurité numérique

Plusieurs mesures de sécurité seront déployées dans les prochains mois :

- Mise en place de la double authentification pour l'accès à nos outils numériques.
- Déploiement d'un gestionnaire de mots de passe pour renforcer la sécurité de nos comptes.
- Révision et renforcement global de nos équipements de sécurité, parmi lesquels : nos pare-feu, antivirus, et systèmes de sauvegarde...



Conclusion

Je tiens à saluer chaleureusement tous les acteurs de notre collectivité pour leur engagement et leur professionnalisme tout au long de cette transformation numérique. Nous avons tous relevé le défi de moderniser nos pratiques, de renforcer notre efficacité opérationnelle, et de garantir une meilleure gestion de nos données.

Je suis pleinement conscient que cette transition représente un changement significatif dans nos habitudes de travail. Chaque contribution, chaque effort individuel et collectif a été crucial pour avancer vers une organisation plus connectée, plus sécurisée, et plus efficiente.

La mise en place des nouveaux outils et des nouvelles règles de fonctionnement, bien que parfois déroutantes, nous permet de mieux coordonner nos activités, de sécuriser nos informations, et de continuer à offrir un service de qualité à nos usagers.

L'adoption de la PSSI simplifiée par le conseil municipal marque une étape importante dans notre engagement pour la cybersécurité. Elle fournit un cadre clair pour nos actions futures et démontre notre détermination à protéger nos systèmes d'information et les données de nos citoyens.

Ensemble, nous avons montré que nous sommes capables de nous adapter et de surmonter les défis imposés par l'évolution rapide des technologies et les exigences de sécurité accrues. La sensibilisation aux risques de cyberattaques, la formation continue, et la préparation de notre Plan de Continuité d'Activité sont des étapes essentielles pour garantir la résilience de notre collectivité face aux menaces numériques.

Nous devons poursuivre sur cette voie, en maintenant nos efforts de collaboration et en restant vigilants quant à la sécurité de nos systèmes et de nos données. Nous pouvons non seulement assurer la continuité de nos services, mais aussi améliorer la qualité du service rendu à nos usagers, en tirant pleinement parti des outils numériques à notre disposition.

Continuons à travailler ensemble avec la même détermination et le même esprit d'innovation, pour faire de notre collectivité un exemple de modernité, d'efficacité et de sécurité numérique.

Le Maire d'Arcadie,