ANTENNE RÉGION VALAIS ROMAND

I.1 : CHARTE UTILISATEURS ET GESTION MATÉRIELLE DES RESSOURCES INFORMATIQUES

Les prestataires IT de la commune restent les interlocuteurs de référence pour cette thématique.
Cette fiche doit être considérée comme indicative et n'est en aucun cas exhaustive.

Pour des raisons de lisibilité, sauf mention spécifique, toute dénomination de personne, de statut ou de fonction se rapporte aux personnes des deux sexes.

CONTEXTE

Il est nécessaire de se prémunir d'un sinistre numérique. L'origine d'une attaque informatique peut être externe (phishing, site Internet, etc.) mais également interne (mot de passe faible, clé USB dérobée, documents papier oubliés, etc.).

En prévention à ces vulnérabilités humaines, organisationnelles et techniques, l'exécutif communal doit veiller à la sécurité de ses ressources informatiques. Une attention toute particulière sera également portée au matériel physique qui est souvent laissé pour compte par les communes. Seule une approche globale de la sécurité (cyber et physique) permet d'éviter les intrusions et ainsi de limiter l'accès à des documents confidentiels ou sensibles par des personnes non autorisées.

QUI ?

Exécutif communal

L'exécutif a la responsabilité de garantir la sécurité du stockage et du transfert des données personnelles des citoyens auprès d'une autre autorité. Il est donc nécessaire que le parc informatique de la commune réponde à des normes minimales en matière de sécurité informatique et physique des infrastructures afin de minimiser les dégâts en cas d'attaque (cyber ou physique) ou d'incident majeur.

Opérationnel communal

Le garant de la Charte utilisateurs doit être impérativement désigné à l'interne. Selon les circonstances et les ressources, ce rôle peut être assigné à un employé administratif et devrait, idéalement, être **indépendant** du service informatique afin d'éviter tout conflit d'intérêts. Une formation niveau **CFC d'employé de commerce** convient pour la bonne exécution de ces tâches qui requiert des compétences administratives, de l'entregent et idéalement de bonnes connaissances en informatique. Le garant de la Charte utilisateurs s'assure **ponctuellement**, mais de manière **régulière**, que la thématique de la sécurité numérique et physique est abordée en continu auprès des salariés de la commune.

POINTS DE CONTRÔLE

- ☐ Nous avons formellement désigné un collaborateur en charge de l'application et du respect de la Charte utilisateurs.
- ☐ Nous avons une **Charte utilisateurs** et tous les salariés de la commune en ont pris connaissance et l'ont signée.
- ☐ Nous avons une politique de gestion et d'utilisation des périphériques privés et du matériel informatique dans le cadre du travail à distance.
- ☐ Nous connaissons les composants de notre réseau informatique ainsi que les prestataires informatiques y relatifs.

ACTIONS PROPOSÉES

1. Nommer un garant de la Charte utilisateurs et le communiquer aux salariés de la commune

Un interlocuteur a été clairement identifié comme étant le garant de la Charte utilisateurs. Cette personne se tient à disposition des collaborateurs pour répondre aux questions relatives à l'application de la Charte utilisateurs qui définit les règles et les limites d'utilisation des ressources informatiques communales.

2. Créer une Charte utilisateurs et s'assurer de son adoption

La création d'une Charte utilisateurs permet de fixer un cadre collectif et de diminuer les risques informatiques. Elle est un gage de responsabilité et de confiance pour les parties prenantes et fera notamment mention des modalités en lien avec la connexion sur un réseau et de l'interdiction de connecter des périphériques privés (clé USB, disque dur externe, etc.). Un **comportement responsable et vigilant** doit être attendu de la part des salariés communaux lors de l'utilisation des infrastructures informatiques communales et privées afin de limiter le risque de cyberattaque et d'incident majeur. L'adoption d'une Charte utilisateurs permet de définir un cadre et de responsabiliser les collaborateurs de l'administration notamment dans le cadre du travail à distance (incluant le télétravail et le travail de milice). L'annexe I.1.I vous propose un exemple de Charte utilisateurs qui peut être adaptée aux besoins de la commune.

ANTENNE RÉGION VALAIS ROMAND

I.1 : CHARTE UTILISATEURS ET GESTION MATÉRIELLE DES RESSOURCES INFORMATIQUES

Les prestataires IT de la commune restent les interlocuteurs de référence pour cette thématique.
Cette fiche doit être considérée comme indicative et n'est en aucun cas exhaustive.

Pour des raisons de lisibilité, sauf mention spécifique, toute dénomination de personne, de statut ou de fonction se rapporte aux personnes des deux sexes.

ACTIONS PROPOSÉES (SUITE)

3. Adopter une politique claire d'utilisation des périphériques privés ainsi que du matériel informatique lors du travail à distance

Avec la démocratisation du télétravail, il est fréquent que les utilisateurs utilisent leurs équipements personnels dans un contexte professionnel et vice versa. Cette pratique augmente les risques en matière de sécurité des données (perte ou fuite de données, sauvegardes non sécurisées, intrusions…). Il est vivement conseillé de **séparer les usages personnels et professionnels**. En d'autres termes, il faut éviter de connecter des équipements privés aux ressources informatiques de la commune, car cela augmente la probabilité de transmission d'un programme malveillant, y compris pour le personnel de milice. **L'annexe I.1.II** propose des recommandations minimales visant à réguler l'utilisation des périphériques privés dans le cadre du travail à distance.

Deux cas de figure doivent être envisagés :

1er cas

Idéalement, la commune fournit au personnel de milice un équipement informatique sécurisé (supports amovibles de sauvegardes, VPN, etc.) et crée les comptes d'accès aux différents logiciels nécessaires à l'accomplissement des tâches prévues dans le cadre de sa fonction. La gestion du matériel informatique est entièrement administrée par la commune notamment lors du départ d'un milicien, elle a la responsabilité de réinitialiser l'ordinateur portable, de formater les supports amovibles et de supprimer les différents accès (serveur, cloud, etc.) et comptes utilisateurs.

2e cas

Le personnel de milice utilise son ordinateur privé dans le cadre de sa fonction publique. Il suit les recommandations et directives de la commune notamment celles mentionnées à **l'annexe I.1.II**. La commune lui fournit des outils de sécurité minimum tels qu'un accès VPN et un support amovible professionnel (clé USB, disque dur, etc.).

4. Connaître et maîtriser son réseau et WIFI communal

Votre réseau informatique communal est un élément essentiel de votre système d'information et de communication avec les habitants communaux. Si votre réseau informatique est mal sécurisé, il peut être aisément utilisé à des fins malveillantes et vos données peuvent être facilement interceptées. En matière de cybersécurité et de performance, l'installation filaire reste plus adéquate. En cas de méconnaissance de votre système réseau communal, il est conseillé de contacter votre prestataire IT afin de procéder à un audit de sécurité de votre réseau informatique. Cette thématique est abordée dans la fiche O.3 sur la cybersécurité. L'annexe I.1.III fournit un aperçu d'un réseau informatique « type » et des points de contrôle à avoir.

ANNEXES

I.1.I : Charte utilisateurs
I.1.II : Fiche de gestion des périphériques privés
I.1.III : Réseau informatique communal et gestion du WIFI
I.1.IV : Actions proposées et discussion avec votre prestataire IT

ANTENNE RÉGION VALAIS ROMAND

I : CHARTE UTILISATEURS

Les prestataires IT de la commune restent les interlocuteurs de référence pour cette thématique.
Cette fiche doit être considérée comme indicative et n'est en aucun cas exhaustive.

INFORMATIQUE & TÉLÉPHONIE

La charte utilisateurs permet non seulement de définir les conditions d'utilisation des ressources informatiques, de téléphonie et d'internet, mais aussi de **responsabiliser** les salariés de la commune vis-à-vis de la sécurité numérique et de la confidentialité des données.

Modèle de Charte utilisateurs

Art. 1 GÉNÉRALITÉS

1.1. Sauf mention spécifique, toute dénomination de personne, de statut ou de fonction se rapporte aux personnes des deux sexes.

1.2. Le bien-être et la santé du collaborateur restent une priorité. Dans tous les cas, le bon sens doit primer.

1.3. Ce règlement s'applique à tout le personnel. Il fait partie intégrante du contrat de travail.

Art. 2 BUT

2.1. Le but du présent règlement est de définir les droits et les devoirs des utilisateurs à propos des moyens de communication (internet, messagerie électronique, téléphonie) et des postes de travail et autres outils informatiques mis à leur disposition dans le cadre professionnel, de prévenir une utilisation abusive de ces derniers et de régler les conséquences d'éventuels abus.

Art. 3 RESPONSABILITÉS

3.1. L'exécutif communal est responsable de la sécurité informatique et chargé de l'application de ces directives et de ces contrôles.

Art. 4 UTILISATION

4.1. Poste de travail et stockage des données

4.1.1 Le poste de travail est un élément constitutif du système informatique de la commune. La modification de son contenu et/ou un usage inapproprié peuvent avoir des effets sur le fonctionnement global de l'environnement informatique. Le poste de travail doit être utilisé pour accomplir des tâches professionnelles. Chaque utilisateur est responsable du matériel mis à sa disposition et de l'utilisation des données auxquelles il a accès selon le présent règlement.

4.1.2 Aucune donnée privée n'est autorisée sur le réseau. En aucun cas, la commune ne pourra être tenue responsable de la sauvegarde et de la perte de ces données.

4.1.3 Une utilisation privée des applications installées sur le poste de travail est admise exceptionnellement, en dehors du temps de travail, dans la mesure où elle ne constitue pas un abus, notamment qu'elle ne surcharge pas l'infrastructure informatique (stockage ou transfert de fichiers) et ne viole pas le devoir de fidélité et de diligence du collaborateur. Des contrôles peuvent être effectués par des personnes habilitées.

4.1.4 Il est notamment interdit de :
- Modifier la configuration matérielle du poste de travail en retirant des composants ou en installant de nouveaux ;
- Modifier la configuration logicielle du poste de travail en retirant des programmes ou en installant des programmes téléchargés depuis internet ou reçus par courrier électronique ou en provenance de toute autre source ;
- Réaliser des développements informatiques sans autorisation.

Une Charte utilisateurs est disponible sur l'extranet de l'Antenne Région Valais romand à l'adresse suivante : **https://www.regionvalaisromand.ch/fr/fiches-thematiques-provisoires-bonnes-pratiques-1813.html**

ou accessible grâce au QR code suivant :

I : CHARTE UTILISATEURS

Les prestataires IT de la commune restent les interlocuteurs de référence pour cette thématique.
Cette fiche doit être considérée comme indicative et n'est en aucun cas exhaustive.

INFORMATIQUE & TÉLÉPHONIE (SUITE)

4.1.5 Les modifications effectuées en violation du chiffre 4.1.4 ci-dessus seront supprimées sans préavis. Dans le cadre de ses activités professionnelles, chaque collaborateur a accès à de nombreuses données confidentielles qu'il s'interdit de rendre accessible et/ou de diffuser par quelques moyens que ce soit à toute autre personne. Cette obligation de confidentialité dépasse la durée du contrat de travail et reste intacte même après la fin des rapports de travail.

4.1.6 Le collaborateur ne consulte, ni ne stocke ou ne diffuse des informations qui, sous quelque forme que ce soit, constituent notamment une participation à un acte illicite ou qui, en particulier, portent atteinte à la dignité de la personne, présentent un caractère pornographique, incitent à la haine raciale ou constituent une apologie du crime ou de la violence.

4.1.7 Le collaborateur reçoit un identifiant et un mot de passe qui lui sont propres et qui ne doivent être communiqués à quiconque. Ils correspondent à une signature informatique et engagent la seule responsabilité de son détenteur.

4.1.8 Le collaborateur s'engage à ne pas désactiver les protections.

4.1.9 De manière générale, le collaborateur stocke ses données sur les serveurs prévus à cet effet. Il est tenu de les épurer régulièrement.

4.1.10 Le collaborateur verrouille son poste de travail lorsqu'il quitte sa place de travail. En cas d'absence prolongée (plus d'une heure), le collaborateur quitte sa session. A la fin de la journée de travail, il éteint son poste de travail.

4.2. Portables, matériel informatique mis à disposition du personnel

4.2.1 Chaque collaborateur qui reçoit un ordinateur portable avec différents accessoires informatiques en est responsable. Ce matériel reste propriété de l'employeur.

4.2.2 Ce matériel sert aussi pour les séances à l'extérieur et est sous la responsabilité du collaborateur qui en prend soin et signale tout dégât ou problèmes rencontrés. Son usage est réservé pour des activités professionnelles uniquement et il est strictement interdit d'y télécharger des programmes ou d'en laisser libre accès à des tiers non-collaborateurs de la commune.
En cas de vol ou de perte avertissez immédiatement le service informatique.

4.2.3 Aucune donnée déposée sur ce portable n'est sauvegardée et ces appareils peuvent être régulièrement repris pour des raisons de maintenance. L'employeur ne peut être tenu pour responsable de la perte de données suite à cette opération.

4.2.4 Ces portables sont équipés de logiciels permettant l'accès à distance sur les serveurs de la commune. La connexion ne peut être obtenue que sur demande auprès de la hiérarchie ou des ressources humaines, et pour une période définie. Cet accès doit absolument être utilisé de manière restrictive, car il ouvre la porte aux données internes de la commune et ne doit pas être laissé sans surveillance (verrouillage de la session en cas d'éloignement du poste).
Il est fortement recommandé d'activer une double authentification pour les périphériques externes qui doivent accéder au réseau communal. Le collaborateur qui doit effectuer du télétravail doit accepter d'installer sur son téléphone portable les applications nécessaires pour la double-authentification.

4.2.5 L'utilisation abusive de ce matériel, la perte ou la délégation à des tiers de son usage, est considérée comme faute professionnelle grave et passible de sanctions.

Une Charte utilisateurs est disponible sur l'extranet de l'Antenne Région Valais romand à l'adresse suivante: **https://www.regionvalaisromand.ch/fr/fiches-thematiques-provisoires-bonnes-pratiques-1813.html**

ou accessible grâce au QR code suivant:

I : CHARTE UTILISATEURS

Les prestataires IT de la commune restent les interlocuteurs de référence pour cette thématique.
Cette fiche doit être considérée comme indicative et n'est en aucun cas exhaustive.

INFORMATIQUE & TÉLÉPHONIE (SUITE)

4.3. Informatique de gestion

4.3.1 Toutes les données sont à traiter avec confidentialité. Toutes divulgations à des tiers sont proscrites à l'exception du besoin d'en connaître.

4.3.2 L'extraction de données des fichiers à usage autre qu'interne ou strictement professionnel est interdite.

4.4. Internet

4.4.1 Internet doit être utilisé pour la recherche et la diffusion d'informations à but professionnel.

4.4.2 Une utilisation privée est admise en dehors du temps de travail, dans la mesure où elle ne constitue pas un abus, notamment qu'elle ne surcharge pas l'infrastructure informatique (stockage ou transfert de fichiers) ni ne viole le devoir de fidélité et de diligence du collaborateur mais aussi que son utilisation ne constitue pas un dégât d'image pour la commune.

4.4.3 L'employeur se réserve le droit de bloquer l'accès à certaines catégories de sites internet, notamment :

- Sites de transactions financières (notamment les sites boursiers) ou ceux payants ;
- Sites de jeux et de paris ;
- Sites à caractère érotique, violent, raciste ou contraire aux mœurs de quelque manière que ce soit.

4.4.4 Le collaborateur s'engage à ne pas copier illégalement des logiciels, de la musique ou des films, protégés par un «copyright», à ne pas diffuser les informations appartenant à des tiers sans leur autorisation. Il s'engage à mentionner ses sources lors de l'utilisation d'informations.

4.5. Réseaux sociaux

4.5.1 Le collaborateur est invité à relayer et promouvoir les activités de la commune au travers de son activité sur les réseaux sociaux.

4.5.2 Le collaborateur doit en toute circonstance avoir sur les réseaux sociaux un comportement digne et en aucun cas porter atteinte à l'image et à la réputation de la commune ni de ses collaborateurs sous peine de sanctions.

4.6. Messagerie électronique

4.6.1 Messagerie professionnelle
L'utilisation du courrier électronique comme instrument de communication est réservée aux besoins professionnels. Une utilisation privée est admise à titre exceptionnel, dans la mesure où elle ne constitue pas un abus, notamment qu'elle ne surcharge pas l'infrastructure informatique (stockage ou transfert de fichiers) et qu'elle ne viole pas le devoir de fidélité et de diligence du collaborateur.

4.6.2 Messagerie privée (gmail, hotmail, etc.)
L'utilisation d'une messagerie privée, dont l'adresse est autre que utilisateur@commune.ch est interdite sauf si des contraintes techniques l'exigent. Il ne faut pas échanger des courriels professionnels depuis sa messagerie privée.

Une Charte utilisateurs est disponible sur l'extranet de l'Antenne Région Valais romand à l'adresse suivante : **https://www.regionvalaisromand.ch/fr/fiches-thematiques-provisoires-bonnes-pratiques-1813.html**

ou accessible grâce au QR code suivant :

I : CHARTE UTILISATEURS

Les prestataires IT de la commune restent les interlocuteurs de référence pour cette thématique.
Cette fiche doit être considérée comme indicative et n'est en aucun cas exhaustive.

INFORMATIQUE & TÉLÉPHONIE (SUITE)

4.6.3 L'utilisation de fonctionnalités spéciales pour la messagerie est réservée exclusivement à des buts professionnels. Le collaborateur s'engage notamment à ne pas contribuer à la propagation de chaînes de distribution.

4.6.4 En cas d'absence ou de vacances, le collaborateur prend les mesures nécessaires pour assurer un suivi de ses courriers électroniques professionnels. Il active un message d'absence à l'intention des contacts externes et de ses collègues. Chaque collaborateur veille à partager avec tous ses collègues (en lecture) son agenda électronique.

4.6.5 Les fichiers attachés aux mails reçus doivent faire l'objet d'une attention particulière, notamment les extensions : .exe, .com, .bat, .xlm, .vbs, .vb. En cas de doute, il prend contact avec le support informatique.

4.6.6 Le collaborateur s'engage à ne pas diffuser des informations qui peuvent porter atteinte à la réputation de la commune.

4.6.7 Le collaborateur est rendu attentif au fait qu'un courrier électronique peut se transmettre très rapidement et qu'il doit donc être très prudent avec les informations qu'il véhicule, ceci spécialement pour des fichiers attachés à caractère confidentiel.

4.6.8 Si un collaborateur reçoit un courrier électronique à caractère violent, raciste ou pornographique, il doit avertir rapidement le directeur. Ce dernier prendra les mesures qui s'imposent.

4.6.9 En cas d'inscription sur un site, l'adresse courriel du collaborateur peut être utilisée mais il est strictement interdit d'utiliser le même mot de passe que celui de l'accès réseau communal. Il faut privilégier une adresse courriel de service (p. ex. info@commune.ch) plutôt qu'un accès personnel lors de l'inscription à un site ; le cas échéant, consigner les sites et les identifiants pour ses collègues ou successeurs.

4.7. Téléphonie fixe ou mobile dans le cadre professionnel

4.7.1 Le collaborateur perçoit une indemnité forfaitaire mensuelle pour la mise à disposition de son téléphone et numéro personnel à des fins professionnelles. En contrepartie, son numéro sera communiqué et son appareil servira comme routeur pour ses connexions avec le matériel informatique fourni (p. ex. un VPN).

4.7.2 Les conversations privées, pendant le temps bloqué (présence obligatoire), doivent rester brèves et se limiter au cas de nécessité.

4.7.3 En cas d'absence ou de vacances, le collaborateur prend les mesures nécessaires pour assurer la gestion de ses appels téléphoniques professionnels.

Art. 5 DÉPART DU COLLABORATEUR

5.1. Départ

5.1.1 Au départ du collaborateur, et sans disposition expresse contraire, son «adresse de courrier électronique» est immédiatement désactivée.

5.1.2 Le collaborateur prend les dispositions nécessaires à la transmission des informations, sur les fichiers qu'il gérait, à ses collègues et/ou successeurs.

Une Charte utilisateurs est disponible sur l'extranet de l'Antenne Région Valais romand à l'adresse suivante : **https://www.regionvalaisromand.ch/fr/fiches-thematiques-provisoires-bonnes-pratiques-1813.html**

ou accessible grâce au QR code suivant :

I : CHARTE UTILISATEURS

Les prestataires IT de la commune restent les interlocuteurs de référence pour cette thématique.
Cette fiche doit être considérée comme indicative et n'est en aucun cas exhaustive.

INFORMATIQUE & TÉLÉPHONIE (SUITE)

5.1.3 Le collaborateur résilie les abonnements faites aux newsletters et qui utilisent son adresse courriel professionnel. Il prend également les mesures utiles pour transmettre les éventuels comptes et identifiants qu'il a dû créer dans le cadre de ses fonctions.et qu'il doit transmettre à son successeur.

Art. 6 CONTRÔLES ET MESURES DE SÉCURITÉ

6.1. Contrôles et mesures

6.1.1 Le collaborateur est attaché au respect de la vie privée de ses collègues sur le lieu de travail, et ce en respectant la législation sur la protection des données.

6.1.2 L'exécutif communal se réserve le droit d'accéder à n'importe quel moment à l'ensemble des composants du système, afin d'assurer sa protection et celle des collaborateurs ou afin de déceler des activités illégales.

6.1.3 L'exécutif communal se réserve le droit de procéder à des contrôles anonymes et aléatoires des fichiers. Le traitement des données relevées est confidentiel et soumis à la protection des données.

6.2. Traitement des informations

6.2.1 En cas d'abus constaté, soit lorsque le présent règlement est violé, le président ou le responsable informatique se réserve le droit de faire procéder à des analyses nominatives des fichiers

6.3. Instances compétentes et sanctions en cas d'abus

6.3.1 Après avoir entendu le collaborateur et s'il s'avère que l'utilisation d'internet et des moyens informatiques constitue une violation du présent règlement, l'exécutif communal prend les mesures appropriées pouvant aller jusqu'au licenciement pour justes motifs. Si les agissements du collaborateur sont de nature pénale, l'employeur se réserve tout droit d'agir en justice.

Ainsi adopté par l'exécutif communal du jj.mm.aaaa.

Président

Vice-président

Une Charte utilisateurs est disponible sur l'extranet de l'Antenne Région Valais romand à l'adresse suivante : **https://www.regionvalaisromand.ch/fr/fiches-thematiques-provisoires-bonnes-pratiques-1813.html**

ou accessible grâce au QR code suivant :

ANTENNE RÉGION VALAIS ROMAND

I : CHARTE UTILISATEURS

Les prestataires IT de la commune restent les interlocuteurs de référence pour cette thématique.
Cette fiche doit être considérée comme indicative et n'est en aucun cas exhaustive.

INFORMATIQUE & TÉLÉPHONIE (SUITE)

INFORMATIQUE & TÉLÉPHONIE

Règlement et directives sur l'obligation de confidentialité et sur l'utilisation des outils informatiques, d'internet, de la messagerie électronique et de la téléphonie fixe ou mobile pour le personnel de commune.

Mme/M. : _____

né(e) le : _____

confirme avoir reçu, lu et approuvé le règlement susnommé. Il/Elle s'engage à en respecter les règles et en connaît les conséquences en cas de non-respect de ces dernières.

_____ _____

Lieu, le Signature

DÉPART DU COLLABORATEUR

Selon son contrat de travail, le collaborateur s'est engagé à considérer comme secret professionnel, aussi bien avant qu'après son départ, les informations de toutes natures acquises et relatives à son activité professionnelle au sein de la commune.

Il est interdit de copier et/ou d'emporter tout document (soft, papiers) ou matériel qui a été remis au collaborateur, dans le cadre de l'exercice de son activité professionnelle, lorsqu'il quitte son poste au sein de la commune.

Le/La soussigné(e) déclare avoir respecté ces prescriptions.

_____

Lieu, le

_____ _____

Mme/M. Signature

Une Charte utilisateurs est disponible sur l'extranet de l'Antenne Région Valais romand à l'adresse suivante : **https://www.regionvalaisromand.ch/fr/fiches-thematiques-provisoires-bonnes-pratiques-1813.html**

ou accessible grâce au QR code suivant :

ANTENNE RÉGION VALAIS ROMAND

II : FICHES DE GESTION DES PÉRIPHÉRIQUES PRIVÉS

Les prestataires IT de la commune restent les interlocuteurs de référence pour cette thématique.
Cette fiche doit être considérée comme indicative et n'est en aucun cas exhaustive.

ÉQUIPEMENTS PRIVÉS ET SÉCURITÉ

Travail à distance

Recommandations minimales pour les utilisateurs applicables dans le cadre du :

- télétravail ;
- travail de milice ;
- travail extramuros (séance à l'extérieur, conseil communal, etc.).

1. Connexions sécurisées

- Lors d'une connexion avec votre ordinateur professionnel sur un réseau domestique, il est impératif d'utiliser **un VPN (accès à distance)** – qui est fourni par votre employeur – afin de sécuriser la connexion internet.
- **Modifiez** le mot de passe par défaut de votre réseau WIFI et choisissez un mot de passe utilisant un protocole de chiffrement WPA2 ou WPA3 et non la version WEP qui est considérée comme inefficace.
- Activez la **mise à jour automatique** afin que vos logiciels, vos applications ainsi que votre système d'exploitation soient actuels et donc mieux protégés contre de nouvelles actions malveillantes.
- Ne partagez votre réseau WIFI qu'à des personnes de confiance.
- Pour des raisons de sécurité, évitez de vous connecter sur des WIFI publics (gare, café, etc.), car ces accès Internet ne sont souvent pas sécurisés.

2. Sécurité des données - séparation des appareils professionnels des appareils privés

- N'utilisez pas de Cloud privé ou de stockage en ligne privé pour sauvegarder des données professionnelles.
- Ne stockez pas **des données privées et professionnelles sur le même support** (clé USB, disque dur, téléphone, etc.).
- Votre courriel privé ne doit pas être employé pour transmettre des informations professionnelles et vice versa.
- Utilisez un **protocole de chiffrement** de données lorsque vous sauvegardez des données sur une clé USB ou un disque externe (AxCrypt, Disk Utility, 7-zip, etc.). Votre prestataire IT peut vous conseiller.
- Évitez de connecter **des supports amovibles personnels** sur l'ordinateur professionnel (clé USB, téléphone portable, etc.) et inversement. En cas de nécessité, la commune fournit les supports des sauvegardes (disque dur, clé USB, etc.) qui seront utilisés seulement sur les ordinateurs professionnels.

3. Sécurité physique de votre poste de travail

- Lorsque vous avez terminé votre journée, rangez votre matériel informatique dans un lieu sûr.
- **Verrouillez** manuellement ou éteignez votre ordinateur lorsque vous vous absentez.
- Paramétrez votre écran de veille avec un mot de passe afin qu'il se verrouille automatiquement après (maximum) 15 minutes d'inactivité.
- Générez des mots de passe robustes. L'annexe O.3.II (Fiche d'aide sur les mots de passe) vous indique la marche à suivre pour créer un mot de passe fort.

Pour de plus amples informations, veuillez consulter le site du Centre national pour la cybersécurité :
https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infos-behoerden.html

ANTENNE RÉGION VALAIS ROMAND

I.1.III : RÉSEAU INFORMATIQUE COMMUNAL ET GESTION DU WIFI

Les prestataires IT de la commune restent les interlocuteurs de référence pour cette thématique. Cette fiche doit être considérée comme indicative et n'est en aucun cas exhaustive.

CONTEXTE

Votre réseau informatique communal est un élément essentiel de votre système d'information. Il permet l'échange d'informations entre les postes de travail et les autres composants internes et externes de l'écosystème informatique.

Qu'il soit géré en interne ou fourni sous forme de service par un prestataire IT, une attention toute particulière doit lui être portée, pour des raisons de **performance** et de **sécurité**.

Les risques globaux à considérer sont l'incapacité d'utiliser des ressources internes (impression, gestion des fichiers – tout ce qui est relié au réseau), des **intrusions** dans le système d'information et des **pertes de performance** dues à des composants vieillissants et insuffisamment maintenus.

QUOI ?

Le réseau informatique est composé d'équipements reliés entre eux pour échanger des informations. Un réseau informatique sommaire est composé au minimum des équipements suivants :

Routeur

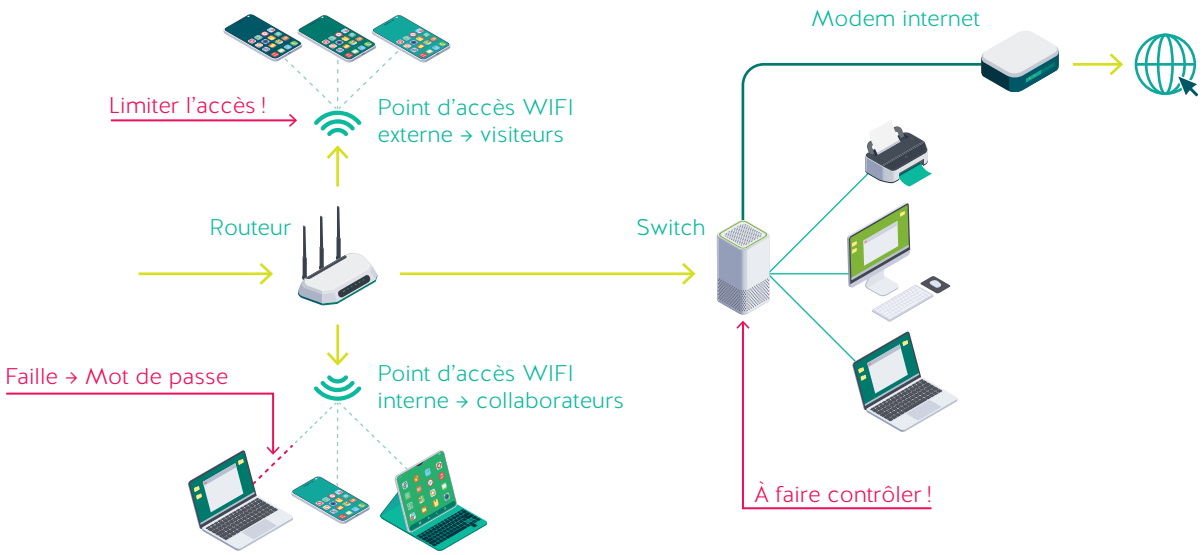
Un réseau est composé au minimum d'un routeur. Il se situe entre internet et votre réseau et permet de fractionner ce dernier en **réseau privé et public de la commune.** Le routeur héberge le pare-feu qui a pour but d'empêcher les accès extérieurs indésirés. Si le routeur est mal géré, il peut présenter des risques d'intrusion, que ce soit d'un sous-réseau à l'autre ou depuis l'extérieur.

Switch

Les switches permettent d'ajouter des appareils sur un réseau câblé en faisant d'un câble plusieurs. S'ils ne sont pas maintenus, des coupures de réseau sont possibles, de même que des phénomènes de vases communiquant non désirés entre deux sous-réseaux, donc d'accès non autorisés à des ressources internes.

Point d'accès WIFI (connexion sans fil)

Le réseau se présente généralement sous 3 formes : un réseau câblé (filaire), un WIFI interne (pour les employés de commune) et un WIFI public (pour les visiteurs). Les antennes WIFI permettent de diffuser du WIFI public ou privé. Elles peuvent présenter des risques de sécurité, p. ex. si les mots de passe de l'appareil et/ou du WIFI ne sont pas assez robustes (cf : annexe O.3.II).



IV : ACTIONS PROPOSÉES ET DISCUSSION AVEC VOTRE PRESTATAIRE IT

Les prestataires IT de la commune restent les interlocuteurs de référence pour cette thématique.
Cette fiche doit être considérée comme indicative et n'est en aucun cas exhaustive.

ACTIONS PROPOSÉES AVANCÉES

Contexte

Dans le cadre de la gestion du matériel du réseau communal, certaines actions peuvent être réalisées par un salarié de la commune ou de concert votre prestataire IT. Veuillez trouver ci-dessous quelques actions concrètes à entreprendre pouvant déboucher sur des discussions avec votre prestataire IT :

1. Connaitre son réseau et le compartimenter

Il est important de déterminer et de vérifier qui a accès à quoi. La décomposition du réseau en sous-réseau permet de cloisonner les accès pour des questions de sécurité (p. ex. un sous-réseau privé pour votre administration, un sous-réseau privé pour votre Police communale, un WIFI public pour les visiteurs ou à la bibliothèque). Assurez-vous d'être en possession d'un inventaire de base, le cas échéant contacter votre prestataire IT. La fiche O.2 aborde cette thématique. Votre prestataire IT pourra également vous aider à compartimenter votre réseau WIFI.

2. Tenir un inventaire des composants du réseau

Avoir une liste des composants du réseau et de leur année de mise en service est nécessaire. Cela vous permet de connaitre vos composants (pas de composants « fantômes ») et de gérer les obsolescences (ce switch a 5 ans, peut-être est-ce lui qui nous cause ces lenteurs, etc.). Un inventaire patrimonial des installations matérielles peut être fourni par votre prestataire IT.

3. Établir un plan de maintenance

Assurez-vous au moins annuellement que les dernières mises à jour sont installées sur les composants réseau. Si vous avez connaissance d'une faille de sécurité sur un de vos composants, il ne faut pas attendre le contrôle annuel pour déployer un nouveau correctif informatique (patch) ou un nouveau pare-feu (firmware). En fonction de la gravité de la faille ou de l'incident, intervenez dans les plus brefs délais ou contactez votre prestataire IT afin qu'il puisse faire le nécessaire. L'annexe A.3.III, vous propose une échelle de gravité et d'urgence.

Il convient aussi de définir des horaires de maintenance pour éviter que des interventions se fassent sur les composants au mauvais moment (p. ex. : lors du bouclement de fin d'année). Il est important de veiller à ce que la configuration d'un composant soit sauvegardée avant sa modification (si le composant ne le fait pas automatiquement) pour pouvoir revenir en arrière si un problème surgit pendant la mise à jour. Enfin, assurez-vous d'être tenu informé des changements nécessaires et effectués. Discutez de la planification de la maintenance avec votre prestataire IT.

4. Monitorer au minimum les changements sur le routeur

Assurez-vous d'être informé automatiquement des modifications (le cas échéant non souhaitées et provenant de l'extérieur) du routeur pour en garder le contrôle.

Et si vous avez d'autres craintes, votre prestataire IT vous accompagnera pour un monitoring plus complet de la performance et des failles de sécurité de votre réseau.

5. Proposition d'actions à mener

1. **Modifiez votre identifiant** ainsi que votre mot de passe qui vous a été attribué par défaut. Pour rappel, l'annexe O.3.II y fait référence.
2. Vérifiez que le protocole de chiffrement sans fil soit en WPA ou WPA-EAS. Le WEP n'est pas fiable et que le pare-feu (firewall) soit activé. Votre prestataire IT peut vous renseigner sur les différents protocoles de sécurité dans fil.
3. **Désactivez votre WIFI** interne lorsque les bureaux sont fermés afin de réduire la probabilité d'une cyberattaque.
4. Vérifiez qui a **accès au compte administrateur** et déterminez dans quelle situation il peut être utilisé, car ce compte permet de réaliser de nombreuses modifications et offre un accès élargi.