ANTENNE RÉGION VALAIS ROMAND

A.3 : GESTION DES INCIDENTS ET DES DEMANDES DE SERVICE

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

Les incidents informatiques sont **inévitables** et n'ont pas tous le même **degré de gravité**. La gestion d'un incident informatique se définit par des processus clairs et des actions concrètes préalablement déterminées par la commune et le prestataire IT.

Un **«incident»** est défini comme une interruption non planifiée (p.ex. une panne) ou la réduction de qualité (p.ex. une lenteur) d'un composant de votre système d'information communal. Il peut empêcher un collaborateur communal d'effectuer son travail correctement (accès bloqué, oubli de l'identifiant, etc.).

Une **«demande de service»** est définie comme une demande utilisateur d'information, de conseil, de changement ou d'accès à un service IT (p.ex. la restauration d'un fichier, un nouveau mot de passe, etc.).

POINTS DE CONTRÔLE

- ☐ Nous avons formellement désigné un collaborateur pour recueillir quotidiennement les demandes de service et les annonces d'incidents des collaborateurs communaux. Il se coordonnera avec le prestataire IT.
- ☐ Nous avons une procédure, même sommaire, permettant l'annonce et la gestion des demandes de service et d'incidents. Cette procédure est connue de tous nos collaborateurs et coordonnée avec nos prestataires IT.
- ☐ Nous sommes au clair avec le mode de traitement des demandes de service et de gestion des incidents par notre prestataire IT. Nous connaissons les délais de réalisation des demandes de service (réinitialisation du mot de passe, création d'un compte d'accès, etc.).
- ☐ Nous réalisons régulièrement (au minimum une fois par année) un **inventaire** avec notre prestataire IT. Ce dernier répertorie les éléments suivants : les délais moyens de traitement des demandes de service et des incidents, leur nombre total respectif, les demandes de service et incidents encore en souffrance et les plus récurrents.

QUI ?

Exécutif communal

L'exécutif est responsable de la planification de toute mesure visant à assurer la continuité de l'activité au sein de la commune. Les demandes de service doivent donc être traitées dans des délais raisonnables. Il en est de même pour la résolution des incidents. À ce titre, l'exécutif supervise ou nomme un superviseur pour la préparation de réponse à un incident informatique, propose des scénarios et s'assure du niveau de service défini contractuellement avec le prestataire IT.

Opérationnel communal

Le gestionnaire d'incident est un collaborateur interne. Selon les circonstances et les ressources, ce poste de travail pourrait même être **mutualisé** avec d'autres communes environnantes. Une formation niveau **CFC d'employé de commerce** convient pour la bonne exécution des tâches qui requièrent des compétences administratives, de la rigueur et de la méthodologie. Le gestionnaire d'incidents s'assure de manière ponctuelle, mais régulière, que les annonces d'incidents et que les demandes de service soient traitées dans des délais raisonnables.

ACTIONS PROPOSÉES

1. Nommer un responsable de gestion d'incidents interne et le communiquer aux collaborateurs

Un interlocuteur de référence doit être désigné et clairement communiqué à vos collaborateurs afin qu'ils adressent leurs demandes de service et annoncent les incidents. Cette personne est le point de contact unique qui se coordonnera avec le prestataire IT. L'annexe A.3.I vous propose quelques exemples de demandes de service et d'incidents informatiques.

2. Utiliser une méthode et une procédure normalisée pour enregistrer les incidents et les demandes de service

Toutes les demandes de service et les incidents doivent être enregistrés (description, date et heure, nom de la personne, service ou composant concerné, etc.). Selon la taille de votre commune, soit dans un outil de «ticketing» communal (proposition de modèle Excel en annexe A.3.II), soit dans le système online que votre prestataire IT vous mettrait à disposition. Le prestataire doit aussi y enregistrer les incidents qu'il détecte lui-même.

Toutes les demandes de service et tous les incidents ne peuvent pas être traités en même temps. Il convient d'appliquer une procédure normalisée (communale ou de votre prestataire IT) pour les prioriser et hiérarchiser. Votre prestataire IT devrait associer un délai de réalisation ou de résolution à chaque priorité. Un exemple de hiérarchisation est présenté en annexe A.3.III de la présente fiche.

ANTENNE RÉGION VALAIS ROMAND

A.3 : GESTION DES INCIDENTS ET DES DEMANDES DE SERVICE

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. Prévoir une procédure spécifique pour les incidents majeurs

On parle d'incident majeur lors d'une interruption significative d'un ou (de) plusieurs services IT. Il nécessite généralement une coordination et une communication (le cas échéant à l'extérieur) spécifiques. On procède alors à une gestion de crise qui réunit au minimum les chefs de services concernés et les collaborateurs en charge des fonctions de gouvernance informatique et des fonctions opérationnelles informatiques. Une liste (imprimée) de contacts prédéfinis peut s'avérer très utile afin de rétablir – dans les plus brefs délais – le bon fonctionnement du parc informatique. L'annexe A.3.IV propose un modèle de liste de contacts.

De concert avec l'exécutif communal et prestataire IT, le gestionnaire d'incidents prévoit plusieurs scénarios qui seront déployés en cas de crise informatique afin d'éviter le chaos. Vous pouvez vous référer à l'annexe O.3.V : Fiche de survie à une cyberattaque.

4. Coordonner les opérations relatives aux incidents et aux demandes de service et faire un point annuel avec le prestataire IT

Le gestionnaire d'incidents doit collecter et consolider toutes les requêtes internes par le biais du registre d'incidents et de demandes de service. L'annexe A.3.II fournit un exemple de **registre sommaire d'incidents et de demandes de service.** S'il constate des récurrences liées aux incidents ou aux demandes de service, il a le devoir de contacter son prestataire IT afin de garantir et d'améliorer l'efficacité du parc informatique communal. À cet effet, un **inventaire annuel** des incidents et des demandes de service sera demandé auprès du prestataire IT ainsi que les délais de restauration. L'annexe A.3.IV fournit un courrier type pour l'annonce d'une demande de service ou d'un incident ainsi qu'un courrier destiné au prestataire informatique pour une demande d'inventaire répertoriant les événements relatifs au parc informatique.

ANNEXES

A.3.I : Exemple d'incidents et de demandes de service
A.3.II : Registre d'incidents et de demandes de service
A.3.III : Hiérarchisation des incidents et de demandes de service
A.3.IV : Courriers types dans le cadre de la gestion des incidents et de demandes de service
A.3.V : Liste de contacts
A.3.VI : Procédure pour annoncer un incident informatique

ANTENNE RÉGION VALAIS ROMAND

I : EXEMPLES D'INCIDENTS ET DE DEMANDES DE SERVICE

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.

LISTE NON EXHAUSTIVE D'EXEMPLES DE DEMANDES DE SERVICE (REQUÊTES INTERNES)

DEMANDE	TYPE DE REQUÊTE	GRAVITÉ DE L'INCIDENT	DÉLAI DE RÉALISATION*
Restauration de fichier(s) ou de répertoire(s)	Demande de service	2	4 heures
Réinitialisation d'un mot de passe	Demande de service	3	1 heure
Création, modification ou suppression d'un espace de stockage	Demande de service	3	2 jours
Demande d'espace partagé	Demande de service	3	3 jours
Changement de nom dans l'annuaire	Demande de service	3	3 jours

** Ces délais sont théoriquement prévus contractuellement par votre prestataire IT. Sinon demandez-lui ses «niveaux de service».*

LISTE NON EXHAUSTIVE D'EXEMPLES D'INCIDENTS (REQUÊTES INTERNES)

DESCRIPTION DE L'INCIDENT	TYPE DE REQUÊTE	GRAVITÉ DE L'INCIDENT	DÉLAI DE RÉALISATION*
Serveur inaccessible pour tous les utilisateurs	Incident informatique	1	4 heures
Perte de données	Incident informatique	1	1 jour
Annonce d'une cyberattaque	Incident informatique	1	2 heures
Tentative de phishing	Incident informatique	2	4 heures

** Ces délais sont théoriquement prévus contractuellement par vos prestataires IT. Sinon demandez-leur leurs «niveaux de service».*

ANTENNE RÉGION VALAIS ROMAND

II : REGISTRE D'INCIDENTS ET DE DEMANDES DE SERVICE

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.

N°	DATE DE L'INCIDENT	DATE ET HEURE DU SIGNALEMENT	AUTEUR DE LA DEMANDE	DEMANDE	TYPE DE REQUÊTE
#1	01.02.23	01.02.23 - 07:00	Monsieur X	Demande d'un nouveau mot de passe	Demande de service
#2	02.02.23	02.02.23 - 10:00	Madame Z	Restauration de fichier(s) ou de répertoire(s)	Demande de service
#3	03.02.23	03.02.23 - 07:00	Monsieur X	Demande d'espace partagé	Demande de service
#4	04.02.23	04.02.23 - 07:00	Madame Z	Changement de nom dans l'annuaire	Demande de service
#5	05.02.23	05.02.23 - 12:22	Madame Z	Création, modification ou suppression d'un espace de stockage	Demande de service
#6	06.02.23	06.02.23 - 00:01	Madame Z	Serveur inaccessible pour tous les utilisateurs	Incident informatique
#7	07.02.23	07.02.23 - 14:40	Monsieur L	Perte de données sensibles	Incident informatique
#8	08.02.23	08.02.23 - 07:00	Madame Z	Tentative de phishing	Incident informatique
#9	09.02.23	09.02.23 - 07:22	Madame L	Annonce d'une cyberattaque	Incident informatique

ANTENNE RÉGION VALAIS ROMAND

II : REGISTRE D'INCIDENTS ET DE DEMANDES DE SERVICE (SUITE)

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.

N°	GRAVITÉ	RÉCURRENCE	DESCRIPTION DE L'IMPACT	PERSONNE À CONTACTER
#1	3	Journalier	Impossibilité de travailler pour un collaborateur	Prestataire IT
#2	2	Mensuel	Impossibilité de travailler	Prestataire IT
#3	3	Mensuel	x	Le responsable du système d'information (RSI)
#4	3	Hebdomadaire	x	Prestataire IT
#5	3	Hebdomadaire	x	Prestataire IT
#6	1	Annuel	Impossibilité de travailler pour tous les collaborateurs	Prestataire IT
#7	1	Mensuel	Problème de confidentialité !	Le délégué à la protection des données (DPO)
#8	2	Mensuel	Risque de perte de données / Intrusion ?	Le délégué à la protection des données (DPO)
#9	1	Exceptionnel	Les habitants ne peuvent plus consulter le site internet	Le délégué à la protection des données (DPO)

Un registre d'incidents et de demandes de service 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

III : HIÉRARCHISATION DES INCIDENTS ET DES DEMANDES DE SERVICE

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.

EXEMPLE DE MÉTHODE NORMALISÉE POUR DÉTERMINER LE DÉLAI DE RÉSOLUTION D'UN INCIDENT

Un problème informatique se traduit non seulement par une complication en lien avec un logiciel ou par un dysfonctionnement du matériel informatique (serveur, imprimante, etc.) mais également par une demande de service telle que l'oubli d'un mot de passe ou la création d'un compte d'utilisateur.

Les **incidents** (voir liste d'exemples en annexe A.3.I) sont annoncés au point de contact unique en précisant qui est impacté et quelle est l'urgence que vous percevez. Le tableau ci-dessous illustre un exemple de calcul de **délai de résolution**, comme le fait un outil de «ticketing». Dans la colonne de gauche sont donnés des exemples de qui est impacté (ampleur de l'impact). Dans la ligne du bas figurent des exemples de notion d'urgence/gravité. En croisant **impact et urgence**, on obtient une priorité qui est ici concrétisée par un délai de résolution.

IMPACT	Blocage dans une situation métier critique	Blocage dans une situation métier importante	Blocage mais attente possible	Pas de blocage
Un seul collaborateur	4 heures	16 heures	5 jours	5 jours
Un groupe de collaborateurs	4 heures	4 heures	16 heures	5 jours
Tous les collaborateurs	2 heures	4 heures	4 heures	16 heures
	1*	2*	3*	4*

URGENCE / GRAVITÉ

** Ces délais de résolution sont théoriquement prévus contractuellement par votre prestataire IT. Sinon demandez-lui ses «niveaux de service».*

Une situation métier critique est par exemple le jour du paiement des salaires ou du bouclement comptable. Une situation métier importante est par exemple une indisponibilité du système d'information alors que de nombreux citoyens font la file au guichet communal. Un incident majeur respectera au minimum les délais de la priorité la plus élevée (le délai le plus court). Ces délais sont théoriquement prévus contractuellement par votre prestataire IT. Sinon demandez-lui ses «niveaux de service».

Lors de la **hiérarchisation** d'incidents informatiques, il est nécessaire de prendre en compte la gravité de l'incident qui est définie contractuellement par votre prestataire IT. Veuillez trouver ci-dessous un exemple **d'échelle de gravité :**

GRAVITÉ	DESCRIPTION	EXEMPLES
1*	Incident critique – fort impact	1 Perte de contrôle de toutes les ressources informatiques 2 Vol ou perte de données confidentielles 3 Intrusion malveillante / cyberattaque
2*	Incident majeur – impact significatif	1 Accès à un serveur impossible pour les collaborateurs de la commune
3*	Incident mineur – faible impact	1 Perte de mot de passe 2 Lenteur du système 3 Solution temporaire (alternative) possible
4*	Demande de service – peu ou pas d'impact	1 Restauration d'un fichier 2 Réparation d'une imprimante réseau 3 Création, modification ou suppression d'un espace de stockage 4 Demande d'espace partagé 5 Changement de nom dans l'annuaire

ANTENNE RÉGION VALAIS ROMAND

IV: COURRIERS TYPES DANS LE CADRE DE LA GESTION DES INCIDENTS ET DE DEMANDES DE SERVICE

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.

EXEMPLE DE COURRIEL POUR L'ADMINISTRATION COMMUNALE

Objet: Annonce de demande de service – réinitialisation du mot de passe

Bonjour Monsieur le Gestionnaire d'incidents ou Monsieur Le Prestataire IT,

M. Administratif n'a plus accès à sa session et il s'agirait de réinitialiser son mot de passe dans les plus brefs délais. Merci de le contacter au +41 07X XXX XX XX et de procéder à une vérification d'identité usuelle.

Je vous remercie pour votre retour et reste à disposition pour toute question supplémentaire.

Meilleures salutations.

Objet: Demande d'inventaire des incidents et des demandes de service pour l'année aaaa

Bonjour Monsieur Le Prestataire IT,

Dans le cadre de l'inventaire annuel de notre parc informatique et en vue de son amélioration, nous aimerions la liste des incidents et des demandes de service pour l'année aaaa incluant les critères suivants:

- La date d'annonce par le collaborateur;
- La gravité de l'incident ou de la demande de service;
- La date de restauration effective ou estimée si pas encore réalisée;
- Une description succincte des mesures prises.

Je vous remercie pour votre support et reste à disposition pour toute question.

Dans l'attente de vos nouvelles, veuillez recevoir, Monsieur Le Prestataire IT, nos salutations les meilleures.

ANTENNE RÉGION VALAIS ROMAND

V : LISTE DE CONTACTS EN CAS D'INCIDENT INFORMATIQUE OU DE DEMANDE DE SERVICE

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.

LISTE DE CONTACTS EN CAS D'INCIDENT INFORMATIQUE OU DE DEMANDE DE SERVICE

Contexte

Pour que la continuité de l'activité de la commune soit garantie, les incidents et les demandes de service doivent être signalés dans les plus brefs délais. Il est donc conseillé de créer **une liste de contacts** proactivement afin de réduire les délais d'intervention. Cette dernière définit le rôle des différents acteurs internes ou externes.

Note : cette fiche doit être imprimée et conservée en lieu sûr afin de garantir l'accès à cette information si le réseau informatique est inaccessible !

Exemple de liste de contacts

QUI ?	ORGANISATION	RÔLE	COORDONNÉES
Le responsable du système d'information (RSI)	interne / ou externe	Gestion des incidents	Information pour contacter la personne (n° de téléphone, courriel, durant le week-end, suppléance, etc.).
Le délégué à la protection des données (DPO)	interne / ou externe	Gestion de la protection des données	
Prestataire IT	externe	Gestion des serveurs	
Monsieur le gestionnaire d'incidents	interne / ou externe	Gestion des incidents	
Monsieur Internet	externe	Fournisseur Internet	

Une liste de contacts 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

VI : PROCÉDURE POUR ANNONCER UN INCIDENT INFORMATIQUE

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.

PROCEDURE A SUIVRE PAR LES COLLABORATEURS LORS D'UN INCIDENT IT

Contexte

En vue d'une constante amélioration des ressources informatiques de la commune notamment en matière de cybersécurité et de réactivité, il est impératif que tous les incidents informatiques soient signalés immédiatement au gestionnaire d'incidents. Dans ce cadre, vous trouverez un exemple de notice que les collaborateurs communaux pourront utiliser pour annoncer les incidents informatiques au responsable d'incidents.

EXEMPLE DE NOTICE A TRANSMETTRE AUX COLLABORATEURS POUR ANNONCER UN INCIDENT IT

Objet : Envoi d'une requête interne / annonce d'un incident IT ou demande de service

Chers collaborateurs,

Dans le cadre de votre activité professionnelle au sein de la commune, vous serez sûrement amenés à faire face à des incidents informatiques ou à faire une demande de service tels que :

- La perte de données ;
- Une tentative de phishing ;
- Un serveur inaccessible ;
- Un compte bloqué – demande d'un nouveau mot de passe ;
- Etc.

Veuillez signaler tous les événements indésirables en contactant le gestionnaire d'incidents si possible par courriel ou par téléphone :

Monsieur le Gestionnaire d'incidents
Gestionnaire.dincident@help.ch
+41 7X XXX XX XX

L'annonce d'incident doit inclure les informations suivantes :

- Heure et date de l'incident : heure ; jj.mm.aaaa
- Description succincte de l'incident
- Impact de l'incident : (interne / externe)
- Mesure (s) prise(s) :
- Autres commentaires :

Je reste à disposition pour toute question supplémentaire.

En vous remerciant de votre collaboration, veuillez recevoir, Mesdames, Messieurs, mes salutations les meilleures.