# CONTEXTE

En cas de panne de courant ou de black-out, il n'est pas possible d'avoir accès aux documents numériques, aux données ou aux moyens de communication habituels. Comme l'ont annoncé certains fournisseurs d'accès à Internet, le réseau de communication et d'accès à Internet ne peut déjà plus être garanti en cas de coupure partielle du réseau, ce qui entraînerait probablement un effondrement du réseau dans toute la Suisse. C'est également le cas en situation de blackout. Comme il n'est plus possible d'accéder aux données ou aux programmes informatiques qui ne sont pas stockés localement sur des réseaux alimentés avec des solutions de secours (génératrice ou réseaux en alimentation propre), il faut prendre les mesures nécessaires.

De plus, déjà en cas de **contingentement**, des analyses montrent que les Datacenters ne seraient pas en mesure d’atteindre les baisses de consommation électrique imposées sans arrêt d’une partie des prestations informatiques, avec les conséquences qui en découlent pour les services métiers impactés.

Afin de se préparer à une telle situation, il est nécessaire que les communes **se déterminent sur les services prioritaires qui doivent absolument être maintenus**, **garantissent que les sauvegardes continuent d’être effectuées** **et** **assurent un accès continu aux données les plus importantes.**

*La commune dispose d’un aperçu des données informatiques qu’elle traite. L’Exécutif communal a sélectionné les données vitales et les conserve dans un format accessible (imprimés ou disque dur externe avec réseau de secours). Les contacts nécessaires ont été pris avec les prestataires informatiques et les mesures adéquates anticipées.*

*Sinon -> Etablir une préparation minimale selon les recommandations ci-dessous.*


# PROCESSUS INFORMATIQUES

**Concrètement ? Quelles sont les actions minimales à entreprendre ?**

Afin d'être préparé au mieux à une situation de crise, les actions suivantes peuvent être entreprises. S’agissant d’une tâche éminemment technique, souvent déléguée à des prestataires externes, il faudrait en premier lieu rencontrer les différentes parties prenantes aux questions informatiques de la commune. Ce groupe de réflexion pourrait être composé, par exemple, du responsable IT de la commune, de l’Exécutif communal, d’un représentant de l’administration (secrétaire communal par exemple), ainsi que du ou des prestataire(s) IT de la commune.

* La première étape est de lister et de définir :
	+ Les **outils informatiques** dont la commune a besoin pour réaliser son travail ;
	+ Les **données** dont la commune a besoin pour réaliser son travail quotidien, ainsi que pour assurer les activités minimales cas de pénurie (par ex. liste des personnes à risque, PCA communal, registre des habitants, etc.) ;
* Corréler les horaires de sauvegardes avec les horaires prévus de délestage (dès que ceux-ci seront connus, notamment via le SIG cantonal ou les gestionnaires de réseaux de distribution). Si une sauvegarde est faite à une heure précise, la faire manuellement avant toute coupure prévue (délestage) ;

*=> Techniquement et selon les systèmes utilisés, il est possible de rajouter un onduleur type UPS qui est connecté à un serveur de type « NAS ». Cet onduleur comprend une batterie et peut tenir environ 1 heure. S’il remarque qu’au bout de 10 / 15 minutes il n’y a pas eu de remise du courant, il va faire une sauvegarde.****Attention, vérifier que l’onduleur soit compatible avec le système informatique utilisé par la commune*** *;*

* **Une fois les sauvegardes terminées, éteindre les systèmes informatiques non secourus avant une coupure de courant prévue (de type délestage) !**

# Suite… : PROCESSUS INFORMATIQUES

* Si la commune procède à des sauvegardes sur des serveurs externes (p. ex. Infomaniak), il serait préférable en cas de suspicion de coupure de courant prochaine de dupliquer les dernières sauvegardes de toute modification également en interne. En effet, il se pourrait que face à une heure fixe de délestage de nombreux clients d’un même service tentent de diriger de manière simultanée trop de données au même endroit, provoquant possiblement une perte de données ;
* **Éclaircir avec les prestataires IT externes à la commune quelles sont leurs stratégies précises face à une pénurie d’énergie.** **Attention : tous les prestataires IT des communes du Valais romand ont des Datacenter décentralisés** (Sierre, Sion, Lausanne et Crissier => en cas de délestage, ça n’est pas seulement la zone de la commune qui compte, mais également les zones où les Datacenters se situent !). En particulier, quels services ne seront plus accessibles ou auront un fonctionnement perturbé, à quels moments, et quelles assurances que les data center (vos données !) seront protégés d’un arrêt brutal du réseau électrique (quels backups prévus, type génératrice, réseau en îlot, etc.), quels temps de remise en service d’un serveur externe, respectivement d’un réseau communal après un délestage ou après un blackout, etc. ;
* Anticiper une collaboration efficace entre les services communaux et l’état-major de conduite (EMC/R). Selon les préparatifs effectués, l’EMC/R pourrait avoir un réseau IT limité, mais fonctionnel. En pratique, **copier les données importantes sur des disques dur ou les serveurs internes de la commune** afin de garantir un accès à ces dernières en cas de crise (! il serait toutefois illusoire de vouloir copier toutes les données de la commune en local !).
	+ Attention : l’accès aux données de la commune peut se faire via des logiciels métiers (cityzen, abacus, etc.). S’assurer qu’au moins un ordinateur du système de secours en soit équipé ;
	+ Attention : C’est une solution qui permet d’accéder aux données « en urgence », mais si on commence à les modifier, il faudra s’assurer de les remettre sur le serveur principal une fois la crise terminée. Afin de ne pas avoir différentes versions des données, il est - de manière générale - préférable d’éviter de modifier des données officielles sur un disque dur externe qui n’est pas synchronisé avec le système principal ;
	+ Attention : Anticiper les besoins énergétiques « IT communal » et prévoir les réserves de carburant (génératrice) en conséquence, ainsi qu’un poste de travail adéquat dans le poste de commandement ;
* Si les données sont conservées localement (NAS, disque dur externe, etc.), garder physiquement les lieux de stockage (les alarmes et caméras ne fonctionneront pas). Le risque de vol de données (par exemple vol d’un disque dur) est plus élevé ;
* **Imprimer les documents importants** afin de s'assurer que ces informations soient accessibles en cas de black-out (penser aux documents nécessaires à la gestion de crise, tels que personnes à risque, surveillance des dangers naturels, points de contacts, fréquences radios, codes d’accès spécifiques, etc.) ;
* **Attention** : Ce n’est pas parce que les serveurs et les ordinateurs portables sont approvisionnés en électricité (réseau de secours) que l’on a forcément accès aux données : il y a souvent des Switch et des routeurs qui assurent la communication entre les serveurs et les ordinateurs portables. Pour que le système fonctionne, ils doivent tous être alimentés ;
* Diminuer les aérations et les températures des serveurs au minimum afin de faire des économies d’énergie.

 **Notes libres : Ma stratégie envisagée / mes points d’attention et de préparation :**

….

# INFORMATIONS GÉNÉRALES / PARTENAIRES

Y a-t-il des partenaires externes dont vous êtes dépendants pour assurer cette activité pendant une panne de réseau, respectivement une crise énergétique ? Si oui, spécifier lesquels, se renseigner si leurs services peuvent être garantis et, le cas échéant, réfléchir à une stratégie de remplacement.

**Identifier tous les chaînons nécessaires au bon fonctionnement de cette activité et s’assurer de leur solidité !**

 **Mes partenaires externes identifiés et mes éventuelles stratégies de remplacement :**

….

# COMMANDES & PRÉPARATIFS ÉVENTUELS (page à transmettre à qui de droit)

**PROCESSUS INFORMATIQUES :**

*Planification / commande des ressources matérielles / humaines & notes diverses*

**Ressources humaines particulières à planifier / informer / former :**

* …
* …
* …
* …
* …
* …

**Achats particuliers à effectuer afin de mener à bien la stratégie identifiée :**

* …
* …
* …
* …
* …

**Champ libre / remarques diverses :**

…

 **Nom, prénom et fonction** :…………………………………………………………………………

**VALIDATION :** La préparation pour cette activité est considérée comme (à reporter dans Excel) :

* Atteinte (*prêts*)
* Partiellement atteinte
* Non atteinte (*pas prêts*)

 **Date & signature** : ………………………………………………………………………….