

Plan de reprise d'activité (PRA)

Qu'est-ce qu'un plan de reprise d'activité (PRA) ?

Un plan de reprise d'activité se définit comme un ensemble de procédures, dont l'objectif est de prévoir comment redémarrer le plus rapidement possible l'activité professionnelle en cas d'incident informatique (catastrophes naturelles, accidents humains, panne matérielle ou logicielle, vol, cybercriminalité, etc...).

Par extension, le PRA désigne également le document recensant ces procédures.

Ce document et les procédures détaillées doivent être accessible en cas de sinistre. Un exemplaire est disponible dans le bureau du responsable informatique et un deuxième exemplaire est disponible dans le coffre du service des Finances. La liste des mots de passe nécessaires pour remettre les systèmes opérationnels étant compris dans ces documents imprimés, ils sont confidentiels et nécessitent d'être gardés sous clé.

Ce présent document est vivant et doit évoluer et se compléter avec l'évolution des services informatique.

Rôle et responsabilités

La liste des responsabilités, les données de contacts en cas d'urgence (professionnelles et personnelles) font partie du document [Composition de la cellule de crise cybersécurité.xlsx](#).

A partir de janvier 2024 la convention de cybersécurité Canton-Commune entrera en vigueur et les coordonnées de contacts de la cellule de crise que cette convention prévoit seront ajoutées à ce document.

Un document regroupant toutes les entreprises auprès desquelles l'administration communale d'Aigle a un service est regroupé dans le document [Contacts.docx](#).

Identification des risques

Les risques sont nombreux et variés. L'analyse de risque a regroupé ces risques en quatre catégories dans le document d'analyse de risques.

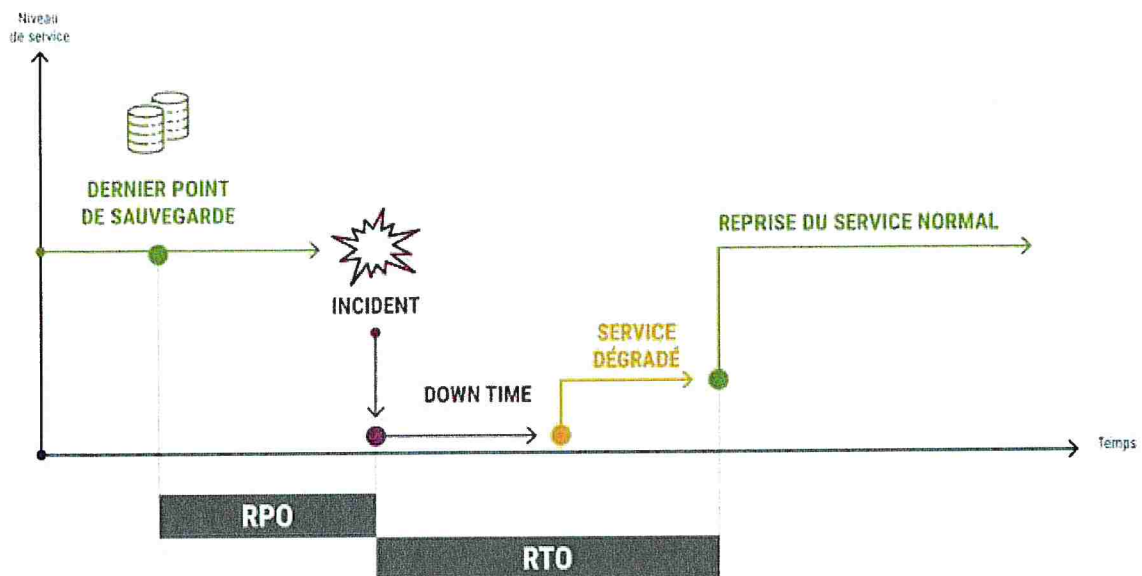
1. Catastrophe naturelle
2. Défaillance du système
3. Humains malveillants
4. Données et configurations

Cette liste, maintenue dans l'analyse de risque, est vivante et doit régulièrement être mise à jour avec les nouveaux risques potentiels. L'analyse de risque est disponible dans le document [Analyse de risque.xlsx](#) et [Risques résiduels.xlsx](#).

Ces risques, et les conséquences qui en découlent, doivent être couverts par une procédure de reprise d'activité adaptée.

En fonction de la nature de l'incident, le RTO, Recovery Time Objective ou la durée maximale d'interruption peut fortement varier. Par exemple un serveur dont un programme interne rend indisponible le service demandé sera beaucoup plus vite disponible que si un des local serveur est cambriolé.

Le RTO est parfois impossible à maîtriser entièrement, il en va ainsi pour les services hébergés chez les partenaires comme la téléphonie. Des solutions de redondance doivent être prévues.



Le RPO, Recovery point objective, soit la durée de perte de données maximale admissible est de 24 heures. Les sauvegardes démarrent après les journées de travail ainsi que le samedi et le dimanche.

Stratégie de reprise d'activité

Prioritairement, il faut le plus rapidement possible que la personne constatant l'incident avertisse un membre de la cellule de crise, si possible le responsable informatique.

En communiquant régulièrement à l'ensemble du personnel de l'existence de ce document et de la cellule de crise, cela accélère la transmission de l'information aux bonnes personnes.

En fonction de la gravité de l'incident, le responsable informatique convoque ou non la cellule de crise. Un vol ou une perte de données est systématiquement communiqué à la cellule de crise.

L'emplacement des actifs ainsi que la liste de ceux-ci sont décrits dans le document

- Données de la commune d'Aigle et leurs emplacements.xlsx

Les droits d'accès aux données, par sources sont décrits dans les documents

- Accès Citizen, compta, Salaires, habitants, votation.xlsx
- Accès site conseil communal cc-aigle.ch.docx
- Accès Système de gestion de l'eau Aquapilet.docx
- Accès Wedo.docx
- Fichier des permissions groupes - dossiers.xlsx
- Fichier liste des groupes de sécurité - utilisateurs.xlsm

Les procédures détaillées sont régulièrement mises à jour en fonction de l'évolution des solutions matérielles et logicielles. Sont décrit dans une procédure les actions à entreprendre dans les cas suivants :

- Panne - coupure de courant.docx
- Panne - application interne.docx
- Panne - Internet.docx

- Panne - plus de téléphonie.docx
- Panne - serveur de fichier Z.docx
- Panne - service d'impression.docx
- Panne - autres pannes hotel de ville.docx
- Panne - machine à affranchir Neopost Quadrant.docx
- Panne - mediatheque.docx

Priorité à respecter en cas de restauration complète

La priorité va à la sécurité des données personnelles que l'administration communale doit gérer.

Ces données doivent être restaurées en priorité dans un environnement sain.

Le réseau informatique doit donc être scanné en premier afin de déterminer s'il persiste un risque pour les données.

Les machines virtuelles doivent être restaurée dans l'ordre suivant :

1. SCAIBAK02 – serveur de sauvegardes, pour lancer les restaurations depuis VEEAM.
2. SCAIDC01 – Contrôleur de domaine sans lequel il n'y a pas de réseau interne.
3. SCAIRP01 – Proxy server contrôlant le flux provenant d'internet à destination de services internes.
4. SCAIAPP06 à 01 – Applications métier Office de la population, Finances, SI, Votations, GED, etc.
5. ESEANCES – Suivi des séances de la Municipalité.
6. DMGeonis – serveur données QGIS données service technique.
7. SCAIFM01 - serveur Filemaker hébergeant des applications développées en interne.
8. DM – serveur d'application barrière déchetterie et KABA.

Révision de ce document

Ce document doit être revu au minimum deux fois par année et à chaque changement impactant sur les procédures de restauration des données et des services informatiques communaux.