

# Prévention des urgences : des plans à géométrie variable



# Responsabilités / Risques

## Responsabilités des institutions patrimoniales

- Préserver, conserver le patrimoine
- Mettre à disposition, communiquer\*
- Evaluer, collecter, classer et décrire, conditionner, conseiller, valoriser



## Risques de plus en plus diversifiés

- Incendie, inondations
- Coupure électricité
- Cyberattaque
- Tremblement de terre
- Conflits



Question : Lesquels faut-il prendre en compte ? Comment?

# 1 - Identifier les risques



- Analyser les risques ou niveaux de risques acceptables
- Définir les risques à limiter, ceux pour lesquels on veut tenter d'apporter une réponse

En ce qui concerne les documents, les agents de détérioration sont:

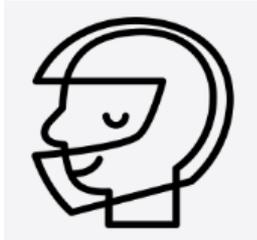
- Forces physiques (dommages sur les documents : déchirures etc.)
- Vol, vandalisme
- Feu
- Eau
- Ravageurs (insectes, rongeurs etc.)
- Lumière, ultraviolets, infrarouge
- Polluants
- Humidité relative inadéquate
- Température inadéquate

<https://www.canada.ca/fr/institut-conservation/services/agents-deterioration.html>

# Elaborer un plan pour limiter certains types de risques



- Se préparer
- Limiter les risques en prenant des mesures préventives
- Diminuer l'ampleur des dégâts pour éviter si possible la perte complète de documents / informations



- Réduire l'effet de la panique
- Aider les professionnels à réagir efficacement en définissant les responsabilités des différents intervenants et en proposant des solutions selon le type de sinistre

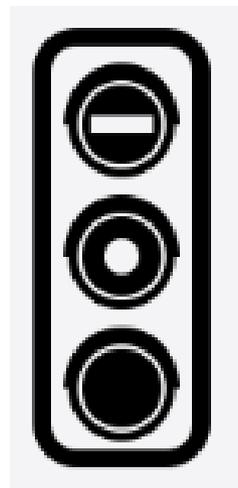


- Permettre à l'institution de continuer à assumer ses missions et maintenir son fonctionnement

# Disposer d'un plan pour chaque type de sinistre et chaque étape

- > **Plan d'évacuation des personnes et plan d'alerte**
- > **Plan de sauvetage**
- > **Plan de rétablissement**

# Prendre des mesures préventives



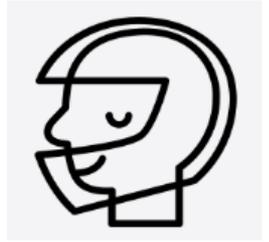
## *Concernant les lieux de stockage :*

- Choisir des locaux qui présentent le moins de risques possibles et les aménager de manière adéquate
- Mettre en place des systèmes de contrôle de sécurité (ex.: détecteurs)
- Selon les risques spécifiques des lieux, mesures spécifiques

## *Concernant les objets :*

- Elaborer et maintenir à jour un inventaire complet des collections, y compris information de localisation des objets  
Veiller à disposer de l'inventaire sous plusieurs formats
- Conserver les objets de manière adéquate, en fonction de leur taille et de leur support
- Selon les intérêts particuliers de certains objets, mesures particulières (ex: création de copies par numérisation/microfilm et stockage dans des lieux différents)

# Elaborer un plan de sauvegarde ou plan d'urgence



Définir les responsabilités & répartir les rôles à chaque étape

→ QUI :

Définir l'ordre des interventions et des équipes concernées

→ QUAND :

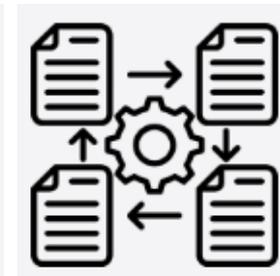
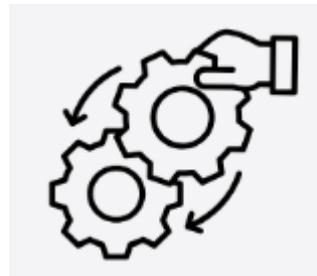
Déterminer quels sont les objets prioritaires

→ QUOI :

Etablir des procédures de sauvetage et de réhabilitation

→ COMMENT :

Acquérir ou identifier le matériel et les ressources nécessaires au sauvetage et à la réhabilitation des collections



# Lors de la déclaration d'un sinistre : Plan d'alerte et d'évacuation

Dans certaines institutions : lever le doute (vérifier ce qui se passe)

- > **Alerter** les services d'urgence
- > **Evacuer**
- > Accueillir et **orienter** les services d'urgence



Lors d'un sinistre, **les corps d'urgence interviennent toujours en premier**  
(Service de défense incendie, gendarmerie, protection civile, protection des biens culturels)

# 1.1 - Alerter et évacuer

Dans tous les cas, il faut que les 1<sup>ers</sup> gestes à faire soient clairs :

## → Alarmer les secours

- Liste des N° d'urgence

## → Si nécessaire : Evacuer

- Plan d'évacuation

**ECA**  
Espace Sécurité Assurée

**CONSIGNES GÉNÉRALES**

**En cas d'incendie**

Téléphoner immédiatement au 118.	Combattre le feu avec un moyen d'extinction approprié.
Sortir du bâtiment en prévenant les personnes et trouvant son propre chemin.	Fermer les fenêtres et les portes.
Rassembler vous à l'extérieur.	Attendre, renseigner et guider les secours.

**Si vous ne pouvez pas sortir**

N'allez jamais dans la fumée.	Indiquez votre position au 118.
Protégez votre porte avec de l'eau et un linge humide.	Manifestez-vous à la fenêtre.

**Dans tous les cas**

N'escaladez pas les voies d'évacuation (escaliers, couloirs, escaliers...).	Dans un local enfumé, placez-vous au plus près du sol.
Ne prenez jamais l'ascenseur en cas d'incendie.	

**N° URGENCES : 118 FEU | 144 SANTÉ | 117 POLICE** [www.eca-vaud.ch](http://www.eca-vaud.ch)

### ▼ Comportement à adopter pendant un séisme

Apprenez comment vous comporter de manière appropriée pendant un séisme, à l'intérieur, à l'extérieur et en déplacement.

#### À l'intérieur des bâtiments

Se mettre à l'abri (par exemple sous une table solide).

Prendre garde aux objets qui chutent ou se renversent (par exemple étagères, meubles lourds, téléviseurs, installations stéréo et éclairage) et éviter la proximité des fenêtres et des baies vitrées, celles-ci pouvant se briser.

Ne quitter le bâtiment que lorsque les environs sont sûrs (par exemple après la chute d'objets tels que des tuiles).

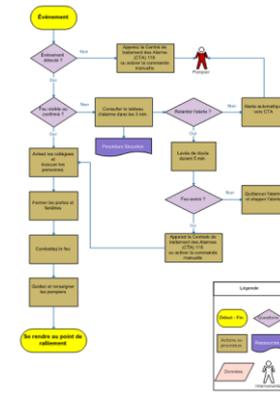
### Conseils en cas de cyberattaque

**COMMENT RÉAGIR EN CAS D'ATTAQUE PAR RANÇONGIER**

En cas de suspicion d'attaque par rançongiciel, des mesures urgentes doivent être prises.

- Isoler votre infrastructure de l'intérieur :** couper les connexions internet, l'accès VPN ou tout autre accès distant.
- S'assurer que vos sauvegardes sont intégrées :** et les dissocier du reste de votre infrastructure. Cela permettra de procéder à la restauration ultérieure des systèmes.
- Contacter la Police cantonale (37) et demander l'aide d'experts pour analyser l'incident :** Cette étape sera votre point de contact avec les autorités cantonales et sera suivie dans son déroulement (après de plainte et première analyse) et impliquera les experts du Centre opérationnel de sécurité vaudois (COSV) en cas de nécessité.
- Une cellule de crise doit être mise en place :** si cela est possible avec, au minimum, un responsable de la communication, un responsable informatique et une personne avec des compétences en cybercriminalité.
- S'appuyer sur un partenaire spécialisé :** en invitant MapInfo qui pourra vous aider dans la gestion technique de l'incident de cybersécurité. La sollicité de vos fournisseurs, via les journaux de connexions logs de vos équipements, sera une des premières étapes techniques effectuées afin de comprendre l'attaque et son origine.
- Annoucer l'incident auprès de la Confédération (INCC) / SINCERT via le site :** <http://www.sincert.ch>

Directeur général de la sécurité et des affaires d'information (DSI) Prévenir en cas de suspicion d'attaque par rançongiciel, article 10 (2) (a) de la Loi fédérale sur la sécurité de l'information (LSI) Pour les professionnels, veuillez nous écrire : [dsi@dsi.ch](mailto:dsi@dsi.ch)



## 1.2 Accueillir les secours et les orienter

Comment est le bâtiment :

- Particularités des locaux et du type de bâtiment

Situation présente :

- De quel sinistre s'agit-il ?
- Où et quand le sinistre a-t-il démarré ?
- Reste-t-il des personnes dans le bâtiment?
- Renseigner sur les priorités : objets à sortir en priorité / mesures spécifiques à prendre dans certains locaux

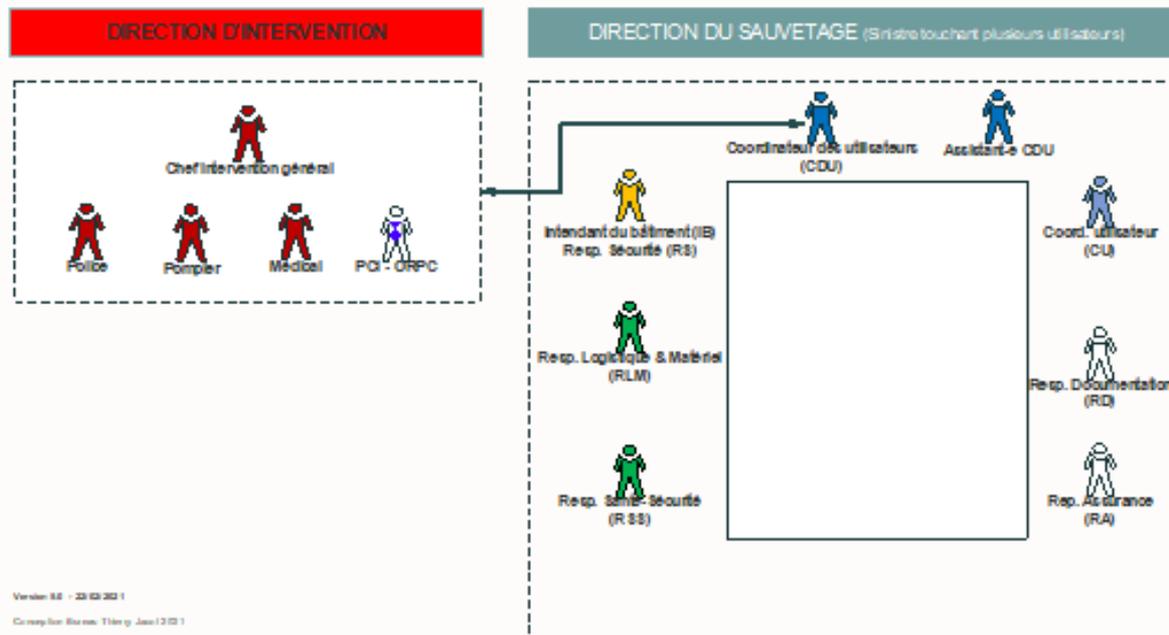
# 1.3 Alerter les personnes concernées

Alerter les personnes concernées :

- Chaîne téléphonique d'alerte (plan d'alerte)

Organiser la prise en charge

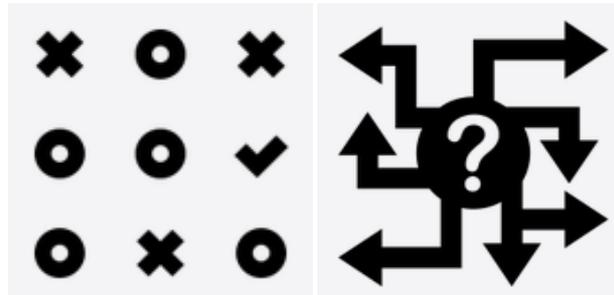
- Liste d'affectation des fonctions
- Descriptif des rôles et missions



## 2 – Evaluer le sinistre et les dégâts

A la fin de l'intervention des services d'urgence

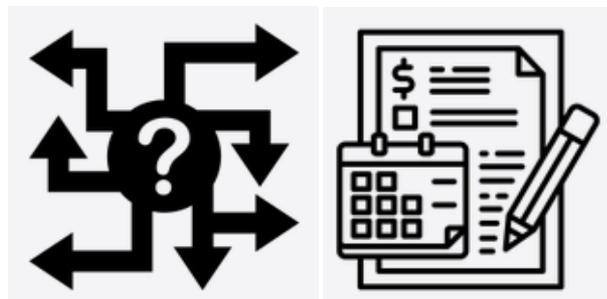
- > Identifier les éléments touchés
- > Evaluer les dégâts
- > Déterminer les mesures à prendre



## 3 – Gérer le sauvetage

Sur la base de la liste établie et des dégâts répertoriés

- > Répartir les actions à mener et confier la responsabilité de chaque action à une personne et petite équipe
- > Initier les actions à mener
- > Planifier le suivi des actions



## 3 – Rétablir le fonctionnement de l'institution

- > Rétablir l'activité de l'institution
  - Plan de continuité : reprendre les activités de base puis progressivement, le fonctionnement habituel de l'institution
- > Continuer de suivre les actions de rétablissement/réparation des documents endommagés
  - cf. projet Heritrack

# En conclusion

- Former les personnes concernées
- Maintenir les documents à jour
- Entraîner régulièrement les premiers gestes (ex.: 4x/an)
- Vérifier l'ensemble de la chaîne des responsabilités et actions par des exercices (ex.: 1x/an)
- Développer le plan en fonction des nouveaux risques identifiés

Merci de votre attention

