Projet Qualité Gestion Des Risques

Construisons ensemble les repères pour sécuriser les organisations

OUTILS POUR LA GESTION DE CRISE



Trame Régionale Plan Bleu

JUIN 2022

LOGO DE L'ÉTABLISSEMENT

Table des matières

Inventaire des équipements et matériels 3
Parc automobile de l'établissement 3
Matériels médicaux 3
EPI 4
Autres besoins 4
Matériel technique : 5
Logistique hébergement 5
II Autres descriptions de l'établissement 6
Gestion des décès 6
III Liste des partenaires 7
Coordonnées des Partenaires : 7
IV Liste des personnels 9
Numéros internes 9
Numéros personnels des salariés 9
V Liste des résidents et modalités de déplacement 10
VI Liste des familles / tuteurs 11
VII Fiche « Sécurité » 12
Sécurisation de l'ESMSS en temps normal 15
A) Analyse des risques 15
B) Evaluation des vulnérabilités 15
C) Procédure de sureté et de sécurité des biens 15
D) Configuration du site 15
E) Signaler les comportements et les situations inhabituelles 15
F) Les numéros utiles 15
Situation en cas de crise 16
A) Comment donner l'alerte ? 16
B) Ressources et moyens de l'urgence 16
C) Procédures d'urgences : 16
D) Conduite A Tenir (CAT) en cas d'attaque terroriste : 17
Les conduites à tenir (CAT) 18

I Inventaire du matériel

Inventaire des équipements et matériels

Listing des équipements et matériels disponibles au sein de l'établissement par grande rubrique (avec possibilité de détailler éventuellement les caractéristiques des matériels et équipements) :

Parc automobile de l'établissement

	Nombre en gasoil	Nombre en essence	Nombre en hybride et électrique
Véhicules particuliers (Administration générale…)			
Véhicules équipés (ambulances ou VSL)			
Véhicules aménagés pour le transport de personnes en fauteuil roulant			
Petits véhicules de transports de personnes (9 pers.)			
Grands véhicules de transports de personnes (>9 pers.)			
Véhicules de transports de marchandise (camion, fourgonnette…)			

Matériels médicaux

Chariot d'urgence	oui/non
Pharmacie	oui/non

	Nombre
Respirateurs de transport	
Respirateurs mixtes	

⇨ Mettre le niveau du stock d'alerte en fonction de chaque établissement

En prévision d'une épidémie, disposer d'un stock équivalent à 3 mois d'une consommation habituelle pour l'ensemble des ressources matérielles citées ci-dessus.

⇨ Mettre le niveau du stock d'alerte	Nombre	Type d'oxygène (liquide, gazeux, pression…)	Nom du fournisseur
Cuves fixes			
Cuves mobiles			
Extracteurs			
Bouteilles			

EPI

EPI	Nombre	Lieu & conditions de stockage	Estimation de la consommation quotidienne en cas d'épidémie
Masques chirurgicaux			
Masques FFP2			
Sur-blouses			
Tabliers plastiques			
Gants			
Lunettes de protection			

Autres besoins

Autres besoins	Nombre	Lieu & conditions de stockage	Estimation de la consommation quotidienne en cas d'épidémie
Solution Hydroalcoolique			
Savon doux liquide			
Boite de mouchoirs à UU			
Rouleaux de sac poubelle			
Rouleaux de papier toilette			
Essuie main à usage unique			

Lieu & conditions de stockage :

PRINCIPES

Stockage sans contact direct avec le sol.
Rangement organisé pour la rotation des stocks.
L'emballage des transports est retiré.
L'emballage secondaire protège l'emballage primaire.

LOCAUX

Volume adapté au stock détenu.
Entretenus et facile d'entretien.
Température ambiante.
Le stock est à l'abri de l'humidité, de la lumière directe du soleil, de dépôt de particules.

ÉQUIPEMENTS DE STOCKAGE

Évitent les surcharges et le risque de chute.
Permettent le stockage dans des emballages secondaires.
Protègent les emballages.
Ne génèrent aucune particule.

Matériel technique :

Stock de sel de déneigement
Pelles, appareil à déneiger…

Logistique hébergement

	Nombre	Lieu
Couvertures		
Lits d'appoints		
Ventilateurs		
Climatiseurs (avec maintenance annuelle)		
Radiateurs d'appoints		
Brumisateur		
….		

II Autres descriptions de l'établissement

Gestion des décès

⇨ **Si crise <u>interne</u>** = voir procédure interne

Si crise <u>externe</u> = voir dispositif ORSAN + « gestion des décès » du Plan ORSEC + se référer aux annonces préfectorales (catastrophes naturelles, technologiques, attentat, épidémie…)

Modalités du constat et certificat de décès (crise interne et externe)

Constat du décès	Certificat de décès
• Seul un médecin sur place peut constater le décès et établir le certificat de décès (pas de téléconsultation, pas de délégation aux directeurs de l'établissements sauf s'il est médecin) • Appeler le médecin traitant du résident ou le médecin traitant habitué à intervenir dans l'établissement ou le médecin coordonnateur	• Les certificats de décès doivent impérativement être remplis de manière lisible, et établis sur des modèles récents conforme à l'arrêté du 17 juillet 2017. • Les formulaires sont disponibles en ligne à l'adresse suivante : https://sic.certdc.inserm.fr

Attention si crise externe : Tenir compte des recommandations régionales ou nationales pour l'appel au SAMU

NB : La loi précise que le certificat de décès est établi par « un médecin, en activité ou retraité, par un étudiant en cours de troisième cycle des études de médecine en France ou un praticien à diplôme étranger hors Union européenne autorisé à poursuivre un parcours de consolidation des compétences en médecine. »

Capacité de conservation des corps

	Nombre	Lieu
Chambre mortuaire		
Chambre réfrigérée		
Lieu réfrigéré		
Housse mortuaire		

III Liste des partenaires

Coordonnées des Partenaires :

Intitulé / Nom	Personne référente	Téléphone général	Ligne directe de la personne référente	Mail de contact
ARS	PFR (Point Focal Régional) H24-7/7	0809 404 900		ars-bfc-alerte@ars.sante.fr
Préfecture				
Mairie				
Gendarmerie/ Police				
Conseil Départemental				
Centre Hospitalier : bureau des entrées				
Centre Hospitalier : urgences				
CPias BFC	Dr N. Floret (NF) I. Rousseaux (IR)	Secrétariat Besançon : 03 81 66 85 57 Secrétariat Dijon : 03 80 29 30 25	NF : 03 81 66 85 50 IR : 03 80 29 30 40	cpias-besancon@chu-besancon.fr cpias-dijon@chu-dijon.fr
Fournisseur d'énergie : électricité (nom)				
Fournisseur d'énergie : autre (nom)				
Fournisseur d'eau (nom)				
Pharmacie partenaire				

Laboratoire départemental				
Laboratoire partenaire				
Prestataire partenaire pour les dispositifs médicaux				
Société de transport (nom)				
Entreprises responsables des différentes maintenances (1 ligne par entreprise : ascenseur, chauffage……)				
Pompes funèbres				

IV Liste des personnels

Numéros internes

Vous pouvez décrire en quelques mots la manipulation à effectuer afin de composer un numéro en interne.

Numéro de poste	Fonction attribuée à ce poste	Nom de la personne titulaire du poste

Numéros personnels des salariés

Cette liste doit être disponible sous pli cacheté dans le document plan bleu.

Nom/ Prénom	Fonction	Site	Téléphone Mobile	Téléphone fixe
….				

Il est important de tenir à jour la liste de ces numéros de téléphone puisqu'elle servira en cas de crise.

V Liste des résidents et modalités de déplacement

NOM, PRENOM DU RESIDENT	CHAMBRE OCCUPEE	MODALITE DE DEPLACEMENT *(AUTONOMIE / FAUTEUIL / CANNE / ALITE)*	ETABLISSEMENT DE REORIENTATION *(LE CAS ECHEANT)*

VI Liste des familles / tuteurs

NOM, PRENOM	NOM ET PRENOM DU RESIDENT/PROTEGE	TELEPHONE	MAIL	ADRESSE

VII Fiche « Sécurité »

Lieu de classement du document		
Historique du document		
Date	**Version**	**Nature des modifications**

Objectif(s)

- Etablir une stratégie de protection en cas d'attaque terroriste et en cas de cybercriminalité

Document(s) de référence

- Instruction du 4 juillet 2017 relative aux mesures de sécurisation dans les établissements et services médico-sociaux
- SGDSN, Organiser un confinement face à une menace terroriste. Fiche pratique à destination des responsables d'établissement accueillant du public ; septembre 2017
- Ministère des Solidarités et de la Santé. Guide « Outil d'auto-évaluation de sûreté - Modèle de fiche de sécurité » ; octobre 2017
- Secrétariat général de la défense et de la sécurité nationale. Faire face ensemble. Vigilance, prévention et protection face à la menace terroriste ; décembre 2016
- CIRCULAIRE MINISTERIELLE N° DGCS/SD2C/2016/261 du 17 août 2016 relative à la préparation aux situations d'urgence particulière pouvant toucher la sécurité des établissements d'accueil du jeune enfant ou des établissements relevant de la protection de l'enfance-
- Service du Haut fonctionnaire de défense et de sécurité. Guide de déclinaison des mesures de sécurisation périmétriques et bâtiments ; juillet 2016.
- Ministère des Affaires Sociales et de la Santé. Vigilance attentats : les bons réflexes. Guide à destination des équipes de direction des établissements de santé, sociaux et médico-sociaux ; juin 2016
- Ministère des Affaires Sociales et de la Santé. Vigilance attentats : les bons réflexes. Guide à destination des personnels des établissements de santé, sociaux et médico-sociaux ; juin 2016

	Rédaction	Vérification	Approbation
Nom(s)			CVS ou structure de participation des usagers équivalente
Fonction(s)			
Date			
Visa			

	Domaine d'application
Personne(s) concernée(s)	
Fréquence d'action	
Lieu d'action : service(s) concerné(s)	

Recommandation(s)
•

Mode d'évaluation
• **Simulation, exercice**

Identification de la structure	
Type d'établissement	
Capacité d'accueil	
Nombre de salariés	
Adresse	
Téléphone	
Responsable de l'établissement	
Responsable de la sécurité et coordonnées et coordonnées	
Coordonnées en cas d'absence du responsable de l'établissement et du responsable sureté	
Coordonnées en cas d'absence du responsable de l'établissement et du responsable sureté informatique	
Identification et coordonnées du correspondant police et gendarmerie	
Identification et coordonnées du correspondant de l'autorité de tutelle	

Sécurisation de l'ESMSS en temps normal

A) Analyse des risques

Risques identifiés	Conséquence sur l'établissement	Degré de priorité de traitement

B) Evaluation des vulnérabilités

Vulnérabilités identifiées	Nature* de la vulnérabilité	Mesure corrective

* Organisationnel, physique ou logique (systèmes d'informations)

C) Procédure de sureté et de sécurité des biens

Nom de la procédure	Lieu de stockage
Gestion des accès	
Réception des plis et colis	
Accueil fournisseurs	
Accueil visiteurs/ familles	
Sortie inopinée (disparition inquiétante)	
Règles d'utilisation des outils informatiques	

D) Configuration du site

Décrire en quelques lignes la configuration de l'établissement (nombre d'accès, nombre de sorties de secours, l'environnement direct de la structure…)

E) Signaler les comportements et les situations inhabituelles

Formaliser auprès de qui signaler ce type de situations : sac abandonné, colis suspect, véhicule suspect, rodeurs…

F) Les numéros utiles

Mettre ici les numéros utiles : direction, gendarmerie, commissariat, pompiers…

Situation en cas de crise

La situation n'est pas figée, elle évolue. Les modes de réaction sont adaptés aux circonstances Dans tous les cas, si une consigne officielle a été communiquée par les forces de sécurité, elle doit être appliquée.
La direction ou son représentant prendra les mesures adaptées à la situation :

- Si l'attaque a lieu à l'extérieur du site, la mise à l'abri peut être préférée à l'évacuation ;
- Si l'attaque a lieu à l'intérieur du site, les mesures d'évacuation ou de mise â l'abri doivent être envisagées en fonction des circonstances et des lieux ;
- Pour envisager une évacuation, il faut réunir 3 conditions :
  - avoir identifié la localisation exacte du danger ;
  - la majorité des personnes présentes sur le site peuvent s'échapper sans risque ;
  - l'alerte a bien été donnée en interne et en externe.

A) Comment donner l'alerte ?

Décrire ici les moyens d'alerte interne à l'établissement : numéros à contacter en priorité, des professionnels à prévenir…
Décrire comment donner une alerte aux services extérieurs : police, commissariat, pompiers…

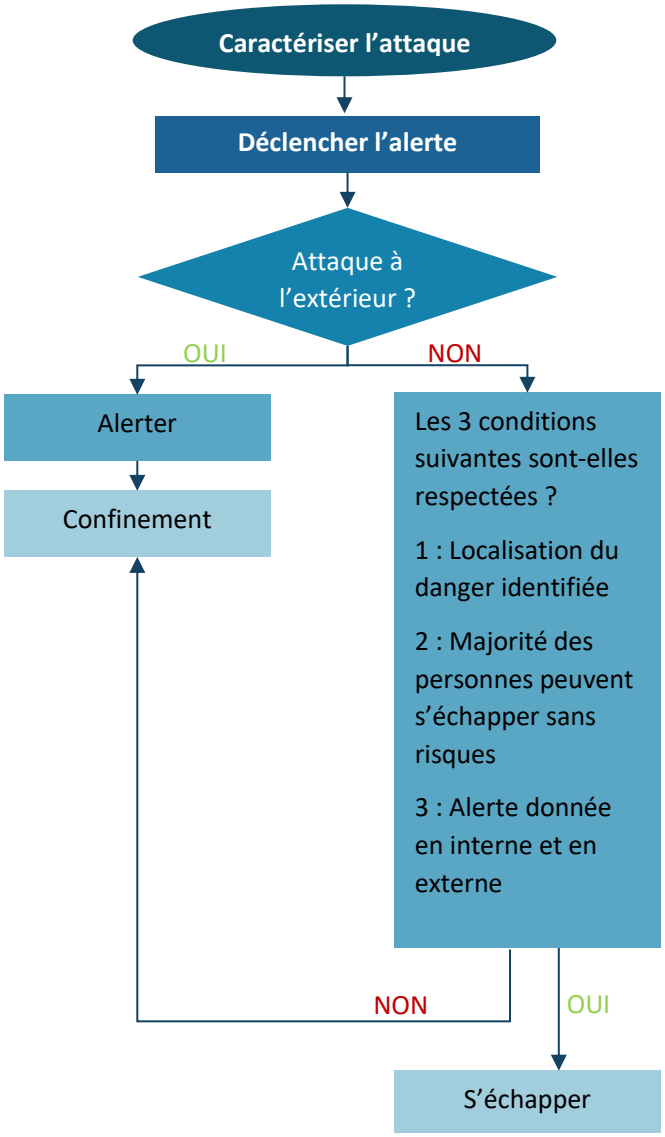
B) Ressources et moyens de l'urgence

Moyens d'alerte	Lieu de stockage
Système d'alarme déclenchant l'évacuation ou le confinement	
Locaux identifiés pour le confinement	

C) Procédures d'urgences :

Nom de la procédure	Lieu de stockage
Activation de la cellule de crise	
Alerter les forces de sécurité intérieures	
Réagir face à un colis suspect	
CAT en cas d'attentat (se confiner ou évacuer, alerter en toute discrétion)	
CAT Alerter	
CAT se confiner	
CAT évacuer	
Réception des plis et colis	
Réagir face à une cyberattaque	

D) Conduite A Tenir (CAT) en cas d'attaque terroriste :

Tous professionnels Concernés		Où ? Quoi (nature de l'attaque) ? Qui ? CAT ALERTER CAT CONFINEMENT CAT S'ECHAPPER

Les conduites à tenir (CAT)

CAT « ALERTER »
Quel message ? Qui appeler ? A Qui Donner le Message ? Comment donner l'alerte ? Quand donner l'alerte ? **Ne pas déclencher l'alarme incendie**

CAT « CONFINEMENT »
1 : Fermer les unités, bloquer les portes ; 2 : Se barricader au moyen du mobilier et des outils identifiés auparavant ; 3 : Eteindre les lumières ; 4 : S'éloigner des cloisons, portes et fenêtres ; 5 : S'allonger au sol derrière plusieurs obstacles solides ; 6 : Faire respecter le silence absolu (mode silence des téléphones) ; 7 : Rester proche des personnes fragiles émotionnellement et les rassurer ; 8 : Attendre l'intervention des forces de sécurité. **NB** : Rester enfermer jusqu'à ce que les forces de l'ordre procèdent à l'évacuation Evacuer calmement les mains ouvertes et apparentes pour éviter d'être perçu comme un suspect Signaler les blessés et l'endroit où ils se trouvent

Lieux de confinement où se cacher dans l'établissement	Outils et mobiliers pour se barricader au besoin	Comportements à avoir dans ce lieu	Missions du professionnel responsable du lieu (le cas échéant)

CAT « S'ECHAPPER »
1 : Rester calme ; 2 : Laisser toutes les affaires sur place ; 3 : Dans la mesure du possible se déplacer à couvert ; 4 : Prendre la sortie la moins exposée et la plus proche ; 5 : Utiliser un itinéraire connu ; 6 : Si possible, aider les autres à s'échapper ; 7 : Alerter les autres personnes autour de vous ; 8 : Dissuader toute personne de pénétrer dans la zone en danger.

Insérer ici un plan des lieux de confinements de l'établissement

NB : Se reporter à la partie « Les procédures incontournables »

Conduite A Tenir en cas de cybercriminalité

En France, la législation punit le cyber piratage et prévoit des sanctions pour ses auteurs. Il ne faut donc pas hésiter à porter plainte dès lors qu'une exfiltration de données ou tentative d'hacking est observée. Attention toutefois : dénoncer nommément une personne même en cas de suspicion peut être perçu comme un acte calomnieux et susceptible de porter préjudice. L'accusé peut à son tour porter plainte en cas de preuves manquantes d'où l'importance de ne mentionner aucun nom dans la dénonciation. En plus de cette mesure, il est également important de laisser les autorités faire leur travail jusqu'à la résolution du problème. Le risque de destruction des preuves indispensables à l'enquête judiciaire est en effet important.

Propositions d'actions de prévention :

- Procéder à une sauvegarde hebdomadaire du serveur et des disques durs
- Mise à jour des antivirus, des différents logiciels…
- Accès « administrateur » à distance pour un nombre réduit de professionnels
- Accès à une messagerie sécurisée en cas d'échanges de données médicales
- Réaliser des bilans quotidiens avec la Direction des Services Informatiques (DSI) et/ou avec les hébergeurs réseaux (FC Net…)

Propositions d'actions en cas de crise :

- Contacter immédiatement la DSI et/ou l'hébergeur
- Constituer des preuves matérielles du cyberpiratage le plus rapidement possible (captures d'écran, mails suspects, numéro de série de l'ordinateur…)
- Dresser une liste détaillée des dommages subis
- Porter plainte auprès du service compétent :

Type d'attaque virtuelle	Instance où porter plainte
Cyber attaque	✓ Commissariat ou gendarmerie de résidence ✓ Service Régionale de la police judiciaire et demander l'enquêteur spécialisé sur la criminalité informatique
Hijack, keylogger, phishiing, spyware, trojan	✓ Office Central de Lutte contre la Criminalité Liée aux Technologies de l'Information et de la Communication (OCLCTIC)
Spams	✓ Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF)
Utilisation frauduleuse de données bancaires	✓ Répression des Contrefaçons des Cartes de Paiement (B.C.R.C.C.P.) ✓ Office Central de Lutte contre la Criminalité Liée aux Technologies de l'Information et de la Communication (OCLCTIC)

Propositions d'actions après la crise **:**

- ✓ Faire un état des lieux de la cybersécurité avec les personnes ressources
- ✓ Faire un RETEX avec la DSI et/ou l'hébergeur

Personnes à contacter en cas de cybercriminalité :

En interne	En externe
Direction (Nom-Prénom-Tel)	ARS (Nom-Prénom-Tel)
Cellule de crise (Nom-Prénom-Tel)	Conseil départemental (Nom-Prénom-Tel)
DSI (Nom-Prénom-Tel)	Hébergeur (Nom-Prénom-Tel)
…	…