Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère des affaires sociales et de la santé

SÉCURISATION DES ÉTABLISSEMENTS DE SANTÉ

GUIDE D'AIDE A L'ÉLABORATION D'UN PLAN DE SÉCURISATION D'ÉTABLISSEMENT (PSE)

1ère édition – avril 2017

DIRECTION GÉNÉRALE DE L'OFFRE DE SOINS

SECRÉTARIAT GÉNÉRAL DES MINISTÈRES SOCIAUX

HFDS HAUT FONCTIONNAIRE DE DÉFENSE ET DE SÉCURITÉ

Avant-propos

Les établissements de santé sont par nature des espaces ouverts au public. Ils accueillent en permanence des patients et leurs proches. Ils sont à ce titre un reflet de la société et sont confrontés à toutes les formes de violence que connait notre population.

Pour autant, les établissements de santé doivent assurer dans leur enceinte la sécurité des personnes et des biens. Cette sécurité concerne aussi bien les personnels de santé que les patients, les visiteurs et les prestataires.

De plus, le contexte de menace terroriste et les récents attentats imposent une vigilance accrue et nécessitent d'assurer, sur l'ensemble du territoire, la mise en œuvre effective de mesures particulières de sûreté au sein des établissements de santé. Les établissements de santé, pivots de la réponse du système de santé sont en première ligne en cas d'attentat terroriste. La continuité des soins étant indispensable, il est donc essentiel de les protéger, notamment contre les menaces de sur-attentat.

Face à ce constat, un plan d'action relatif à la sécurisation des établissements de santé a été élaboré par le ministère des affaires sociales et de la santé, en coordination avec le ministère de l'intérieur[1]. Cette démarche s'inscrit dans le cadre d'une politique globale et pluriannuelle de sécurité des établissements, pilotée par les agences régionales de santé.

Une instruction ministérielle[2] a été diffusée en novembre 2016, qui décline le rôle des agences régionales de santé en matière de coordination de la politique de sécurité dans les territoires et crée l'obligation pour les établissements de santé publics et privés d'élaborer un plan de sécurisation de leur établissement.

L'objectif vise bien à protéger les établissements, tant contre les violences au quotidien que contre la menace terroriste, aujourd'hui multiforme.

Le présent guide a pour objet d'accompagner les établissements de santé dans l'élaboration et la mise en œuvre de leur plan de sécurisation d'établissement (PSE).

Il accompagne les chefs d'établissements dans l'identification des risques et des menaces.

Il décrit et explicite les différents chapitres devant figurer dans le PSE, ainsi que les modalités d'exercices et de révision de ce plan.

Enfin, ce document d'aide se voulant pratique, il comporte des fiches opérationnelles sur la conduite à tenir face à un certain nombre d'évènements.

---

[1] Lettre conjointe des ministres des affaires sociales et de la santé et de l'intérieur relative à la sécurisation des établissements de santé du 16 novembre 2016, NOR : AFSC1633394C

[2] Instruction n° SG/HFDS/2016/340 du 16 novembre 2016 relative aux mesures de sécurisation dans les établissements de santé, paru au BO n°12 du 15 janvier 2017 (p. 199)
http://social-sante.gouv.fr/fichiers/bo/2016/16-12/ste_20160012_0000_p000.pdf

Ce document est le fruit d'une collaboration active, à la fois des professionnels de la santé et des responsables du ministère de l'intérieur en charge du renforcement de la sûreté des lieux publics et privés.

Pour les accompagner dans leur démarche, les chefs d'établissements pourront solliciter l'appui :

- des préfectures et plus particulièrement les services chargés de la sécurité ;
- des forces de sécurité intérieure (FSI) : notamment les correspondants ou référents sûreté de la police et de la gendarmerie et les services spécialisés ;
- des agences régionales de santé : les responsables de la sécurisation des établissements de santé ;
- du ministère des affaires sociales et de la santé ; service spécialisé du haut fonctionnaire de défense et de sécurité hfds@sg.social.gouv.fr et délégué à la sécurité générale de la direction générale de l'offre de soins sante.securite@sante.gouv.fr .

Le secrétaire général des ministères sociaux,
Haut fonctionnaire de défense et de sécurité.

Sommaire

Introduction

Le plan de sécurisation d'établissement (PSE) définit la politique et l'organisation globale pour sécuriser l'établissement. Conçu comme un véritable document structurant pour la sécurité et la sûreté de l'établissement, le PSE se veut un document pratique et doit permettre ainsi à la direction de l'établissement de s'interroger sur des scénarios (tant quotidiens qu'exceptionnels) et d'élaborer des réponses adaptées à la nature des activités et de l'environnement. La réponse à ces scénarios peut conduire à repenser certains dispositifs : qu'ils soient humains, organisationnels ou techniques.

Le PSE constitue le document cadre matérialisant l'engagement de la direction de l'établissement de santé à mener une politique de sécurisation de l'établissement et du personnel.
Ce document est le prolongement du travail d'analyse de risques d'actes de malveillance et de terrorisme et définit les priorités de la politique de sûreté.
Le PSE doit faire sens au regard des enjeux de l'établissement et des ressources qu'il peut y consacrer.

Dans ce cadre, l'analyse de risque doit tenir compte de l'appréciation des impacts, de l'analyse des vulnérabilités propres à l'établissement et de la probabilité de survenue d'événements malveillants.

Il convient d'associer en amont les institutions représentatives du personnel au regard des enjeux portant sur la sécurité et les conditions de travail, a minima sur certains travaux préparatoires du PSE.
Toutefois, il est nécessaire de veiller à ne pas diffuser des informations sensibles. À cette fin, l'accès au PSE finalisé devra être limité : en interne à l'établissement, aux seules personnes ayant besoin d'en connaître ; en externe, uniquement auprès des ARS, des préfectures et des correspondants des FSI. **Le PSE portera une mention « diffusion limitée »**. **Toute publication est formellement à proscrire** sur internet ou sur un intranet ne permettant pas une discrimination individuelle des accès.

Il est important d'élaborer ce PSE en coordination avec les autorités préfectorales et les forces de sécurité intérieure, ces dernières pouvant apporter leur concours à l'élaboration du plan. Les ARS sont également en mesure d'accompagner et de conseiller les établissements dans leur démarche rédactionnelle, en s'appuyant notamment sur leur groupe d'appui technique.

Conformément au décret n° 2016-1327 du 6 octobre 2016 relatif à l'organisation de la réponse du système de santé (dispositif « ORSAN »)[3] et à l'instruction n° SG/HFDS/2016/340 du 4 novembre 2016, tous les établissements de santé sont assujettis à l'élaboration d'un PSE. S'agissant des établissements qui relèvent du secteur d'activité d'importance vitale « Santé », l'élaboration de leur PSE est complémentaire du plan particulier de protection (PPP) de leur(s) point(s) d'importance vitale (PIV). L'élaboration d'un PSE portera en particulier sur les mesures non couvertes par le PPP.

Enfin, pour permettre au directeur d'établissement de réaliser au mieux son projet de sécurisation, les premières actions à mener sont indiquées à l'Annexe n°1 du présent guide.

[3] https://www.legifrance.gouv.fr/eli/decret/2016/10/6/AFSP1617819D/jo/texte

1. Structure du guide

PLAN TYPE DU PSE

PRÉAMBULE – PRÉSENTATION GLOBALE DE L'ÉTABLISSEMENT

Bref rapport de présentation de la localisation de l'établissement et de ses activités
Positionnement sur une carte

CHAPITRE I – ANALYSE DES RISQUES

Description de l'environnement et des particularités de l'établissement
Environnement et fonctionnement de l'ES
Caractéristiques principales de l'ES
Organisation fonctionnelle de l'ES

Risques malveillants pour l'établissement
Identification des risques
Hiérarchisation des risques

Vulnérabilités spécifiques de l'établissement
Identification des points névralgiques
Hiérarchisation des vulnérabilités

Synthèse – plan d'action pluriannuel

CHAPITRE II – SÉCURISATION DE L'ÉTABLISSEMENT EN TEMPS NORMAL

Mesures de prévention
Etablissement d'une convention « santé – sécurité – justice »
Formation, sensibilisation et communication (personnels, patients, sous-traitants, visiteurs, fournisseurs, élèves des écoles et des centres de formation)
Procédures
Surveillance
Prévention de la radicalisation

Mesures de protection
Dispositifs de sûreté en place ou prévus
Zonages, clôtures et obstacles retardateurs
Protection des bâtiments, des accès, des parkings
Contrôle des entrées et des sorties de personnes et de véhicules (employés, sous-traitants, patients, visiteurs, fournisseurs)

Dispositifs de détection d'intrusion
Eclairage
Energie
PC de sécurité
Protection des systèmes d'information, y compris télécommunications
Protection des systèmes de sécurité-sûreté
Alerte
Les systèmes internes à l'établissement
Consignes en cas d'alerte
Systèmes d'astreinte et de permanence
Systèmes externes à l'établissement
Dispositions concernant le personnel et consignes de sûreté
Procédures de recrutement et d'accès des personnes
Relation avec les sous-traitants
Equipes de protection et de gardiennage
Rôle éventuel du personnel des autres branches de la sécurité
Tests et maintenance périodiques du matériel et du personnel de protection

CHAPITRE III – SÉCURISATION COMPLÉMENTAIRE EN SITUATION D'ATTENTAT OU DE CRISE LOCALE

Alerte, communication et information
Dossier d'intervention (*document à verser en annexe*).
Schémas d'alerte (interne et externe).

Renforcement de la sécurisation périmétrique et des accès
Mesures graduelles pouvant être mises en œuvre.

CHAPITRE IV – MAINTIEN EN CONDITIONS OPÉRATIONNELLES DU PSE ET ARTICULATION AVEC LES AUTRES PLANS

Exercices
Organisation retenue pour les exercices de mise en œuvre du PSE

Mise à jour du PSE et des procédures
Date de la dernière version du PSE

Articulation avec les autres plans
Plan Vigipirate
Plan blanc
Plan de continuité d'activité (PCA)

ORGANISATION DES ATTENDUS ET DES COMMENTAIRES

Pour une meilleure compréhension de ce guide, une charte graphique différencie les contenus exigés dans le PSE de ce qui relève de l'orientation ou du commentaire à destination du rédacteur du plan.

Voici, à titre d'exemple, un aperçu de cette identité visuelle et sa signification correspondante :

1. ARCHITECTURE DU PSE	Structure du présent guide
CHAPITRE N – XXXX	Titre de chapitre du PSE (obligatoire)
n. Les sources de menaces et de risques pour l'établissement	Titre de sous-partie (obligatoire)
identification des menaces	Information à mentionner (obligatoire)
Indiquer…	Précision ou information importante
Il s'agit à partir de…	Commentaires et/ou exemples de ce qui peut être renseigné

2. Attendus et commentaires sur le contenu du plan de sécurisation d'établissement

PRÉAMBULE – PRÉSENTATION GLOBALE DE L'ÉTABLISSEMENT

Bref rapport de présentation de la localisation de l'établissement et de ses activités.
Premièrement, indiquer la nature (public, privé, ESPIC) et la localisation de l'établissement.
Préciser la disposition bâtimentaire (monobloc, pavillonnaire ou multisite).
Mentionner le nom et les coordonnées de la personne (ou du service) ayant réalisé le PSE.
Dater la version du PSE.

Au travers d'un positionnement sur une carte, il sera facile de situer l'établissement pour permettre de comprendre dans quel environnement géographique est (ou sont) implanté(s) le(s) bâtiment(s) : milieu rural ou péri-rural, ou au contraire densité du tissu urbain…

Parmi les enjeux du territoire qui seront représentés, doivent figurer les informations environnementales suivantes :

- *points particuliers de cet environnement (proximité d'un site sensible ou SEVESO, d'un établissement scolaire ou d'une administration, etc.) ;*
- *principaux risques naturels locaux ;*
- *interconnections et/ou proximité avec des établissements de santé voisins.*

CHAPITRE I – ANALYSE DES RISQUES

La finalité de ce diagnostic initial est bien de planifier des mesures correctrices adaptées selon un calendrier défini et en fonction des priorités arrêtées par le directeur de l'établissement.

En premier lieu, les forces de sécurité intérieure doivent être sollicitées par le rédacteur d'un PSE pour disposer d'informations sur les risques liés à l'environnement de l'établissement.

Les éléments statistiques utiles en matière de délinquance pourront être récupérés à partir du site internet du ministère de l'intérieur Interstats[4]*.*

Un état des lieux (appelé rapport de physionomie) pourra être demandé en complément auprès de la circonscription de sécurité publique localement compétente (groupements de gendarmerie départementale, directions départementales de sécurité publique de la police nationale ou directions territoriales de sécurité publique de la préfecture de police). Cet état des lieux peut comprendre les éléments suivants :

- *les tendances de la délinquance locale ;*
- *les difficultés particulières rencontrées par les forces de sécurité intérieure sur la zone ;*
- *les lieux ou les périodes les plus criminogènes ;*
- *l'origine endogène ou exogène de la délinquance, ...*

Un entretien avec des représentants locaux des forces de sécurité intérieure pourra également être organisé avec :

- *le correspondant local ou le référent sûreté (police ou gendarmerie) afin d'apporter un appui technique dans le domaine de la sûreté (dispositif de sûreté mis en place et améliorations) ;*
- *le groupement de gendarmerie départementale ou la direction départementale de la sécurité publique concernant la préparation à la gestion de crise.*

Il est important d'établir un échange constructif à vocation pédagogique entre les parties tout au long de la rédaction du PSE pour faciliter la prise en compte de la sûreté.

Pour faciliter les mises en relation, l'établissement peut prendre l'attache de son agence régionale de santé.

[4] http://www.interieur.gouv.fr/Interstats

1. Description de l'environnement et des particularités de l'établissement

Environnement de l'ES

Présenter l'environnement immédiat de l'ES au regard de la sûreté et les interactions entre cet environnement et l'ES. Faire figurer :

- *l'environnement social :*
  - *habitat de type privé, social, collectif, individuel… ;*
  - *composition sociale de la population… ;*
  - *présence de structures sociales, de centres…*

- *l'environnement économique :*
  - *catégories socioprofessionnelles ;*
  - *éventuelles difficultés économiques ;*
  - *activité économique (agricole, industrielle, tertiaire…) ;*
  - *présence de services publics de l'Etat…*

- *un diagnostic de l'insécurité extérieur à l'ES :*
  - *au moyen de données chiffrées (sources diverses possibles dont le site internet du ministère de l'Intérieur Interstats, l'INSEE et des services municipaux ou des opérateurs de transport) ;*
  - *prise en compte du « climat ambiant » : détournements d'espaces, fréquentation nocturne, période de commission des infractions, problèmes rencontrés par les services de sécurité, ... Ces éléments pourront être compris dans le rapport de physionomie.*

- *un bilan de l'insécurité dans l'ES :*
  - *présenter la situation des incivilités et de la délinquance (antécédents marquants, statistiques malveillance, ambiance de sécurité).*

Caractéristiques principales et fonctionnement de l'ES

La description des activités doit permettre d'identifier succinctement la physionomie de l'établissement et ses :

- *superficie, **nombre de bâtiments** (dont ERP, IGH), présence de galeries, zones de stationnement ;*
- *établissement de santé de référence, établissement de 1ère ligne, de recours, de repli ;*
- *description de l'offre de soins, services spécialisés : CRRA 15, SMUR, SAU, accueil de polytraumatisés, plateaux techniques, etc. ;*
- *nombre de lit et/ou volume de patients accueillis annuellement ;*
- *nombre de personnels ;*
- *flux moyens quotidiens piétons et véhicules (personnels, patients, visiteurs, prestataires) ;*
- *toute autre caractéristique ou spécificité méritant d'être soulignée.*

Organisation fonctionnelle de l'ES

Fournir des renseignements portant sur l'organisation de l'ES sous l'angle « sécurité – sûreté ».

- *l'organisation hiérarchique de l'établissement (autorité, responsables, permanence de direction) ;*
- *l'organigramme avec les noms, numéros de téléphone (une mise à jour régulière est indispensable) ;*
- *l'effectif employé (personnels médicaux et paramédicaux, personnels administratifs et techniques, sous-traitants, etc.).*

- *les responsables de la protection du site :*
  - *identification du responsable de la sûreté du site et de son suppléant (préciser les autres fonctions exercées par ces personnes) ;*
  - *identification des structures concernées (sous-traitance éventuelle de certaines fonctions de sécurité) ;*
- *identifier les structures (sous-traitance éventuelle de certaines fonctions de sûreté et/ou de sécurité) ;*
- *la présentation du poste central de sécurité.*

2. Risques malveillants pour l'établissement

Identification des risques

Identifier dans un premier temps l'ensemble des risques potentiels (y compris ceux portant sur l'ensemble des systèmes d'information numériques – SIH, biomédical, gestion centralisées techniques ou bâtimentaires) pesant sur l'établissement.

Une liste de menaces est jointe en* Annexe n°2 *de ce guide, elle constitue une liste minimale des événements susceptibles de survenir devant être étudiés. *Pour compléter cette liste, il faut prendre en compte l'historique des événements de l'établissement (phénomènes de violence, agressions…). Il est indispensable de disposer d'un outil unique tel que la « plateforme-signalement » de* l'observatoire national des violences en milieu de santé[5] *(ONVS) recensant au quotidien tous les événements liés à la violence : interventions du service de sécurité, déclarations d'événements indésirables, accidents du travail. L'ONVS propose une nomenclature de la grille de déclaration ONVS permettant ainsi des statistiques comparées. L'outil doit permettre l'identification précise des causes (prise en charge perfectible, faiblesse des structures…) dans un but d'action.*

Pour adapter au contexte local cette liste, chaque ES pourra échanger avec les acteurs d'autres établissements aux caractéristiques similaires, mais aussi solliciter les forces de sécurité intérieure locales pour connaitre les risques pesant sur l'établissement.

Hiérarchisation des risques

Les risques précédemment listées doivent être priorisées. Pour les classer en fonction de leur criticité, il convient de mener une évaluation qualitative et/ou quantitative des risques identifiés : probabilité (événements vécus ou pouvant survenir), gravité et acceptabilité (incluant la prise en compte des mesures correctrices déjà mises en œuvre par exemple : restriction des accès, etc.).

Une représentation graphique (sous forme de tableau ou de matrice de criticité) doit permettre de lister l'ensemble des risques de l'établissement (Cf. exemple ci-après). ***Chaque établissement a l'entière liberté de choisir sa méthode de cotation pour hiérarchiser ses risques.***

[5] Accessible à l'adresse suivante : https://o6.sante.gouv.fr/oNVS/

Exemple de hiérarchisation des risques

Le tableau ci-dessous reprend un échantillon des menaces présentées dans l'Annexe n°2.
La hiérarchisation ci-après est proposée à titre d'exemple.
Les risques sont classés en fonction de leur vraisemblance, leur impact et l'importance des conséquences qu'ils engendrent.

Cotation	Probabilité	Impact *(dans le fonctionnement de l'ES)*
4 =	**très probable**	gravité **extrême** *(indisponibilité totale et durable de l'ES)*
3 =	**probable**	gravité **majeure** *(indisponibilité partielle et/ou temporaire de l'ES)*
2 =	**improbable**	gravité **modérée** *(perturbation limitée (max. quelques heures d'un service)*
1 =	**très improbable**	gravité **mineure** *(perturbation n'entrainant pas de rupture de fonctionnement)*

Risque = probabilité X impact

Menaces	Probabilité	Impact	Risque
1- Vols sans effraction, dégradations légères, dégradations de véhicules sur parking intérieur de l'établissement.	**3**	**1**	**3**
4- Injures, insultes et provocations sans menaces, chahuts, occupations des locaux, nuisances, salissures.	**4**	**1**	**4**
6- Menaces d'atteinte à l'intégrité physique ou aux biens de la personne, menaces de mort, port d'armes, menaces avec arme par nature ou par destination (arme à feu, arme blanche, scalpel, rasoir, tout autre objet dangereux).	**3**	**2**	**6**
7- Agressions physiques : violences volontaires (atteinte à l'intégrité physique ou psychique).	**3**	**3**	**9**
10- Attaques par des moyens improvisés tel que des véhicules bélier.	**2**	**4**	**8**
11- Attaques par armes de guerre (fusils d'assaut, grenades, lances roquettes).	**3**	**4**	**12**
12- Dépôt ou utilisation d'engins explosifs artisanaux, industriels ou militaires de conception simple ou élaborée, (dans bagages, drones, véhicules…), déclenchement de ceintures explosives par terroristes.	**3**	**4**	**12**

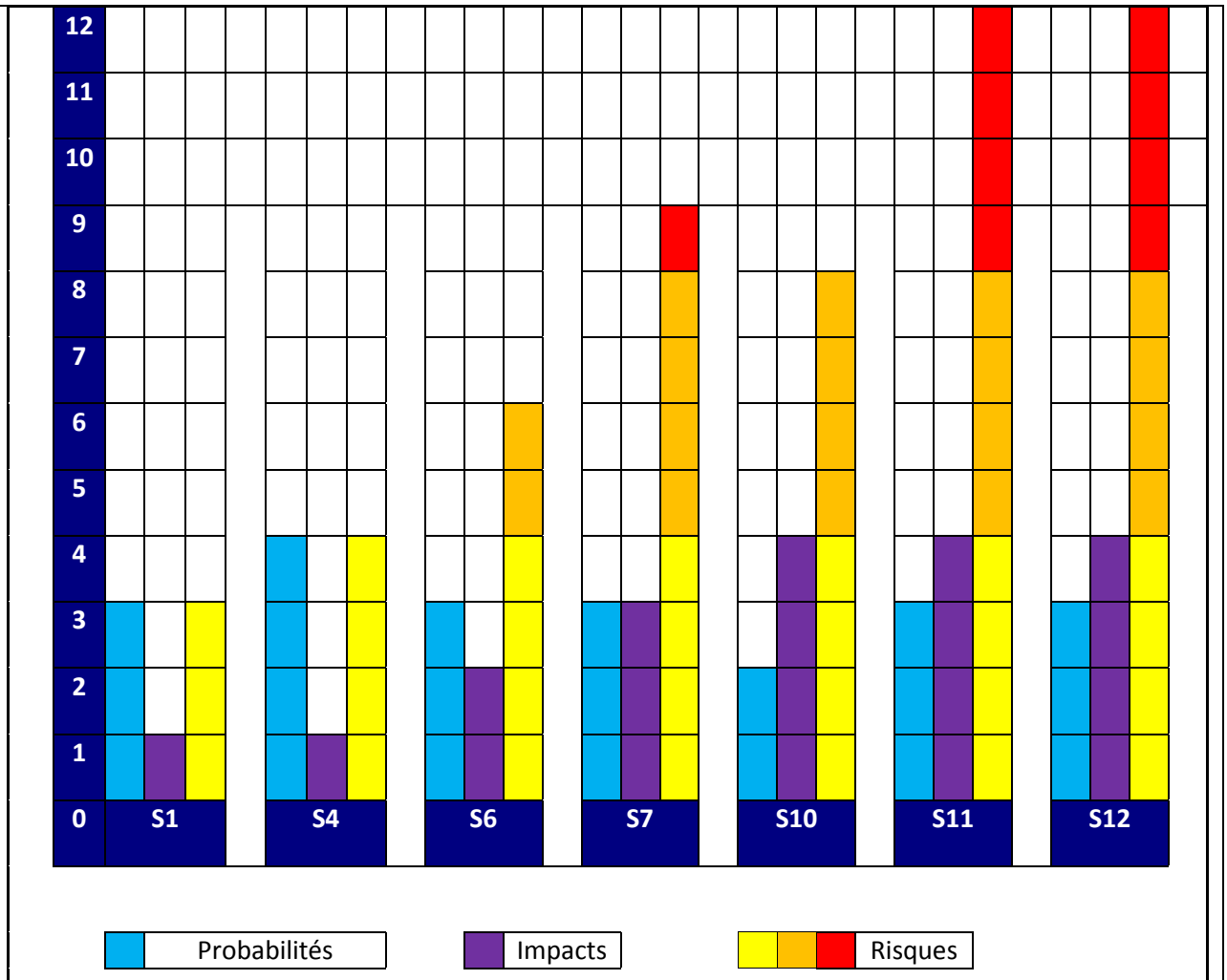

Tableau de synthèse de l'appréciation des risques (mise à jour du xx/xx/2017)

L'analyse des risques ci-dessus permet de constater que quatre scénarios sont à prendre plus particulièrement en considération : prioritairement les scenarios **7, 11 et 12** et le scenario 10.

3. Vulnérabilités spécifiques de l'établissement

Identification des points névralgiques

Chaque établissement comporte un certain nombre de points névralgiques. ***Un point névralgique se définit par l'importance et/ou la fragilité d'un équipement ou d'une activité dont la disparition ou l'arrêt aurait des conséquences importantes sur la capacité de l'établissement à assurer ses missions de soins ou de prise en charge.***

Il est demandé d'identifier dans un premier temps l'ensemble des points névralgiques de l'établissement. Ils doivent être listés notamment en tenant compte de :

- *la mise en évidence des interdépendances (exemple : nécessité de disposer d'une alimentation électrique permanente pour assurer le fonctionnement des systèmes de sécurité) ;*
- *l'influence de l'environnement exposé précédemment dans le document (milieu urbain sensible, multiplicité des sites et des accès, délimitation périmétrique par rapport à l'environnement) ;*

- *la structure organisationnelle de l'établissement (importance et nombre des sous-traitants et prestataires, sensibilisation du personnel à la sécurité) ;*
- *l'exposition aux menaces spécifiques (cf. ci-avant) : actes de violence sur le personnel, occupation illicite de locaux et de lieux (sous-sol, parking, hall), vols, accueil des détenus et des gardés à vue, transport de fonds (régie, lieu de stockage des encaissements avant transfert vers la banque, DAB), etc. ;*
- *les risques techniques : locaux d'entreposage de matériels dangereux (azote, oxygène, etc.).*

Cet inventaire peut être listé ou représenté sous forme de tableau.

Hiérarchisation des vulnérabilités

Certains points névralgiques sont plus vulnérables que d'autres. Ils doivent donc être priorisés. Ce classement est fonction de leur criticité propre et de leur exposition aux risques les plus élevés, identifiés ci-avant.

Il est nécessaire de mener une évaluation qualitative et/ou quantitative des vulnérabilités identifiées : probabilité, gravité et acceptabilité (prise en compte des mesures correctrices déjà mis en œuvre par exemple : restriction des accès, etc.).

Une représentation sous forme de tableau permet de lister l'ensemble des points névralgiques de l'établissement devant faire l'objet d'un plan de traitement.

Modèle de tableau des points névralgiques les plus vulnérables, présenté par ordre de criticité ***(à titre d'exemple, à simple fin d'illustration).***

	Points névralgiques les plus exposés aux risques
1.	Accueil et espaces d'attente des Urgences
2.	Poste Central de Sécurité (PCS)
3.	Hall d'entrée principal
4.	Parking public
5.	Régie financière
6.	Pharmacie centrale
7.	Local EDF et TGBT
8.	Groupes électrogènes
9.	Réseau informatique
10.	Chaine d'approvisionnement (eau, nourriture, etc.)

4. Synthèse – plan d'action pluriannuel

Au regard des risques et des points névralgiques les plus vulnérables, conclure cette analyse en mettant en exergue les mesures prioritaires à prendre, d'ordre humain, organisationnel, et technique.

Lister par ordre de priorité les mesures à prendre et les actions engagées avec ***un échéancier sur 3 ans*** *(durée à titre indicatif). Cette démarche pluriannuelle est gage d'efficacité et permettra de partager avec l'ensemble des acteurs la montée en puissance de la sécurisation de l'ES.*

CHAPITRE II – SÉCURISATION DE L'ÉTABLISSEMENT EN TEMPS NORMAL

Décrire le premier mode de fonctionnement : la sécurisation de l'établissement en temps normal.

Ce mode de fonctionnement reflète le niveau permanent adopté par l'établissement pour faire face aux menaces le visant. Le dimensionnement de cette posture se fonde sur l'analyse de risques du chapitre précédent. L'objectif d'une politique de prévention des atteintes aux personnes et aux biens est de diminuer la fréquence et la gravité des faits.

Il s'agit principalement de décrire les mesures humaines, organisationnelles et techniques mises en œuvre pour assurer la sécurité de tous au quotidien.

***Dans le cadre de l'élaboration du PSE, toutes les mesures de prévention (dissuasion des menaces, résilience) et de protection (défense en profondeur, réaction à un événement) rentrent dans le cadre du présent chapitre**. Ces mesures doivent répondre aux vulnérabilités décrites dans l'analyse des risques ; et inclure aussi des contrôles et des mises à jour réguliers pour maintenir ces mesures efficaces.*

1. Mesures de prévention

Les mesures de prévention intègrent les actions d'anticipation de l'établissement (planification, dissuasion, formation, surveillance/vigilance) pour éviter ou réduire le risque de survenue d'un événement.

- Établissement d'une convention « santé – sécurité – justice »[6]
  Décrire les aspects couverts par cette convention si elle a déjà été établie. Dans le cas contraire, préparer cette convention en y intégrant a minima les éléments suivants :
  - *la coordination de l'action dans le domaine de la sécurité ;*
  - *les procédures d'information de l'autorité judiciaire, notamment du procureur de la République ;*
  - *le diagnostic des situations à risques et des dispositifs de prévention notamment dans les établissements de santé ou les services les plus exposés à des risques d'incivilité et de violence ;*
  - *les modalités d'intervention des forces de sécurité auprès des établissements et des professionnels de santé, ainsi que le renforcement de l'action des établissements en situation de crise ;*
  - *les procédures d'information et sensibilisation des personnels hospitaliers à la prévention et à la gestion des conflits en milieu de santé.*

***NB :** Les conventions déjà établies doivent être mises à jour en incluant un volet terrorisme.*

- Formation, sensibilisation et communication (personnels, patients, sous-traitants, visiteurs, fournisseurs, élèves des écoles et des centres de formation)
  Indiquer les actions déployées pour l'ensemble de l'établissement :
  - *directives générales et consignes particulières selon les spécificités d'emploi ;*
  - *modalités de formation des personnels ;*
  - *sensibilisation du public.*

[6] Protocole d'accord pour la sécurisation des établissements de santé du 10 juin 2010. Pour prendre connaissance du protocole et pour un exemple de convention voir site ONVS .

- Procédures

  Présenter les procédures réalisées ou prévues. Ces consignes formalisées doivent permettre la définition des conduites à tenir en situation normale comme en mode dégradé (notamment la perte de fonction de sûreté telles que la surveillance le contrôle d'accès, etc.).
  A minima, il devra être prévu les mesures :
  - *définissant des zones contrôlées en fonction de leurs activités et de leurs vulnérabilités ;*
  - *communiquant les procédures et les exigences au public, aux fournisseurs, aux sous-traitants et partenaires et vérifiant leur application ;*
  - *établissant des procédures d'identification et de traitement des incidents et des actes de malveillance (peut être traitée au point suivant « surveillance », en fonction du choix du rédacteur) ;*
  - *sélectionnant les lieux de mise en sûreté adaptés pour le confinement ;*
  - *mettant en place un suivi des autorisations d'accès aux locaux réservés et aux informations sensibles (tels que ceux en lien avec les points névralgiques) ;*
  - *élaborant un plan d'évacuation, comprenant notamment les cheminements, l'identification d'issues de secours, les lieux éventuels de rassemblement ou de confinement.*

  Certaines procédures peuvent être élaborées avec les conseils des forces de sécurité intérieure.
  L'organisation du service de sûreté est abordée dans la partie suivante, inutile de l'évoquer ici.

- Surveillance

  Décrire l'organisation mise en place pour recueillir des informations, détecter les incidents et les transmettre. En élaborant ou constituant :
  - *des modes de détection des incidents ou dysfonctionnements internes ou externes susceptibles de constituer des menaces ;*
  - *une chaîne d'alerte et de compte-rendu (service(s) ou personne(s) à prévenir non seulement sur le site mais aussi sans délai les autorités préfectorales, le directeur général de l'agence régionale de santé concernée, et déclaration à l'ONVS).*

- Prévention de la radicalisation

  Décrire l'organisation mise en place pour diffuser de l'information au personnel, détecter les signaux faibles et les incidents et les transmettre. Pour le signalement de cas supposé de radicalisation, voir la Fiche Conseil n°5.

NB : *La mise en œuvre d'une politique en matière de prévention des violences repose sur l'élaboration d'outils de prévention des risques. A ce titre, la DGOS et l'ONVS encouragent les ES à développer leur politique de lutte contre les atteintes aux personnes et aux biens selon trois niveaux de prévention [7]:*

- *la prévention primaire (mesures de dissuasion) : prévenir la violence avant qu'elle ne se manifeste en agissant sur l'environnement et l'organisation ;*
- *la prévention secondaire (mesures de réaction) : mesures immédiates à la violence et la formation à la gestion des situations conflictuelles ;*
- *la prévention tertiaire (mesures de suivi) : se concentrer sur la prise en charge, l'accompagnement et les soins sur la durée après un acte violent.*

[7] http://social-sante.gouv.fr/professionnels/gerer-un-etablissement-de-sante-medico-social/observatoire-national-des-violences-en-milieu-de-sante-onvs/onvs

Exemples de mesures de prévention, adaptables aux risques identifiés

- ***Conception et organisation :***
  - *intégration du paramètre « sûreté » dès l'origine de tout projet, que ce soit dans le projet d'établissement, dans les projets de construction (dès la phase programme) ou les projets de soins ;*
  - *désignation d'un responsable sécurité-sûreté, rattaché directement à la direction, en raison de la confidentialité et de la sensibilité des informations traitées, assurant également le rôle de « correspondant Vigipirate » ;*
  - *mise en œuvre d'une stratégie de sécurité-sûreté dans le cadre de l'application du plan Vigipirate (objectifs permanents de sécurité communs à tous et objectifs de sécurité spécifiques) ;*
  - *association des experts (ressource interne, policiers, gendarmes, secteur privé) en amont des processus de décision pour les problématiques de sécurité-sûreté ;*
  - *développement d'une politique globale de gestion des risques (ISO 31 000…) intégrant les risques professionnels dont font partie les atteintes aux personnes et aux biens ;*
  - *amélioration de l'organisation du travail et de la gestion de la relation avec les usagers (éviter les situations conflictuelles entre le public et le personnel, séparation des flux personnels/patients, mise en place d'une frontière hermétique entre l'espace clinique et l'espace public, transparence des services, gestion du temps d'attente, de la complexité des démarches, retour de l'information vers les patients/résidents et les accompagnants...) ;*
  - *amélioration de l'ergonomie, la propreté, le confort des lieux d'accueil du public, mais aussi de la sécurité des postes de travail et des accès aux locaux de l'établissement ;*
  - *établissement d'un tableau de bord de suivi de la politique de lutte contre les atteintes (document unique…) ;*
  - *mise en place des dispositifs de protection des travailleurs isolés pour les personnels les plus exposés ;*
  - *vérification de la fiabilité et de l'appropriation du matériel de sécurité (s'orienter vers des systèmes au fonctionnement simple, compréhensibles par tous, accessibles et fiables) ;*
  - *réalisation de fiches réflexes en cas d'agressions ;*
  - *réorganisation des circuits d'accueil ;*
  - *établir un règlement intérieur et le diffuser, l'afficher largement.*

- ***Formation, sensibilisation et information (des personnels et du public) :***
  - *formation régulière des salariés et des dirigeants qui doivent maîtriser les procédures de gestion des risques auxquels ils sont confrontés, mais aussi gérer les situations conflictuelles et désamorcer la violence des usagers ;*
  - *identification des personnels référents chargés d'aider leurs collègues à canaliser l'agressivité des usagers, ou d'apporter un accompagnement médico-social, psychologique ou juridique ;*
  - *organisation d'échanges de pratiques entre salariés sur la manière de gérer la relation aux patients et résidents, et notamment les situations tendues ;*
  - *rappel des consignes de sûreté (port du badge apparent, fermeture systématique des portes et issues à la fin des activités journalières non permanentes, etc.) ;*
  - *mise en place de plusieurs niveaux de communication adaptés aux objectifs visés (de la communication sur la prévention à la communication de crise - différencier le court terme du long terme) ;*
  - *établissement d'une information précise et concise à destination des usagers et de leur entourage, mais aussi envers les membres du personnel et permettant la transmission des informations entre médecins, soignants et administratifs ;*
  - *rappel de la politique de sécurité-sûreté (toute mesure nouvelle a été accompagnée d'une communication à l'ensemble des acteurs concernés : le risque existe, les mesures ont été prises pour le prévenir, quel est mon rôle, quels réflexes adopter si un fait se produit malgré tout, qui contacter ?) ;*
  - *mise en place d'une communication spécifique pour l'application du plan Vigipirate et sensibiliser les personnels aux comportements suspects (guide du SGDSN : faire face ensemble, 1er décembre 2016) ;*
  - *afficher dans les différents accueils les règles en vigueur notamment les interdictions auxquelles doivent se plier le public (exemple : pas d'accompagnement des familles dans la zone urgence, etc.) ;*
  - *informer le public de ces règles obligations / interdictions le plus en amont possible, lors des prises de rendez-vous, sur le site internet de l'établissement, brochure… (exemples : arriver en avance aux rendez-vous pour passer les dispositifs de sécurité ; présenter une pièce d'identité et/ou une convocation ; interdiction de bagages dans certaines zones, pas d'accompagnements des familles dans la zone urgence, etc) ;*
  - *diversification des supports de communication en fonction des publics visés : éditoriaux (journal, lettre interne, affiche, brochure thématique, encart dans le livret d'accueil, set de table pour le restaurant administratif…), digitaux (site intranet, mailing, réseaux sociaux…), managériaux (séminaires internes, sessions de formation, réunions d'information, journée porte ouverte…), numériques (écrans d'accueil, téléviseurs) et médiatiques (visites organisées pour les journalistes, points presse, communiqués…) à destination de la presse locale notamment ;*
  - *valorisation des mesures mises en place pour améliorer l'accueil, l'orientation, la qualité de la prise en charge et réduire au maximum l'attente, le stress, l'anxiété, l'énervement des usagers et de leur entourage.*

2. Mesures de protection

L'établissement met en œuvre des mesures spécifiques (effets retardateurs, moyens de protection et d'intervention) pour se protéger et limiter les conséquences d'une attaque.
Il est important de souligner que ces moyens humains, organisationnels et techniques doivent être étudiés par vulnérabilité et non de manière globale.
De même, il devra être porté une attention particulière à la maintenance régulière des dispositifs.

Dispositifs de sûreté en place ou prévus
Identifier les mesures en distinguant la posture permanente de sécurité et les mesures temporaires et graduées de vigilance, de prévention et de protection.
Les modalités et les délais de réalisation de ces mesures sont à préciser.
Les mesures de sûreté se réfèrent notamment, mais pas exclusivement, à la posture permanente de sécurité et aux mesures planifiées VIGIPIRATE dont l'exécution incombe en tout ou partie aux établissements de santé (Il s'agit en particulier de certaines mesures ALR, BAT et SAN, dont la liste est à l'Annexe n°4).

Il convient parmi ces mesures de déterminer à la fois les éléments visibles utiles à la dissuasion, et les processus et moyens de protection de site qui doivent rester confidentiels.

- Zonages, clôtures et obstacles retardateurs
  - *zonage établi selon l'importance et la vulnérabilité des secteurs en adaptant leurs mesures de protection*[8].

- Protection des bâtiments, des accès, des parkings
  - *distinguer les moyens techniques et humains.*

- Contrôle des entrées et des sorties de personnes et de véhicules (employés, sous-traitants, patients, visiteurs, fournisseurs)
  - *description des dispositifs : gardiennage, badges d'accès restrictifs (lieux, plages horaire), accompagnement dans les espaces non ouverts au public… ;*
  - *contrôle des consignes à bagages ;*
  - *contrôle visuel des sacs et des coffres de véhicule (voir la Fiche Conseil n°6).*

- Dispositifs de détection d'intrusion
  - *présentation des dispositifs perceptibles (ex. gardiennage, caméras, portes et fenêtres de sécurité, alarmes…) et des moyens discrets (ex. détection thermique, volumétrique, infrarouge, caméras discrètes...) ;*
  - *dispositions prises pour contrôler l'efficience permanente des dispositifs.*

- Éclairage
  - *efficacité des installations choisies : surface éclairée, déclenchement automatique… ;*
  - *fonctionnement en mode dégradé. De même si des dispositifs techniques anti-intrusion (alarme, blocage de porte) sont reliés sur des dispositifs secourus.*

[8] Pour plus de détails, se référer au guide de déclinaison des mesures périmétriques et bâtimentaires du MCAS.

- Énergie
  - *lister les énergies utilisées, leurs fournisseurs, les solutions de remplacement ;*
  - *pour l'électricité, moyens de production autonomes prévus permettant de poursuivre les activités essentielles en mode dégradé et protection de ces moyens.*

- PC de sécurité
  - *description des moyens matériels et humains et de la sécurité du PC lui-même ;*
  - *fonctionnement en temps normal et en cas de crise.*

- Protection des systèmes d'information et de communication (SIC)
  - *protection des installations et des réseaux utilisés ;*
  - *description des plans de continuité numérique (ou faire un renvoi au PCA si existant) ;*
  - *sauvegardes des données sensibles (systèmes de santé, biomédicaux, gestion technique et de sûreté, tel que la vidéoprotection) ;*
  - *vérification régulière pour prévenir ou circonvenir à un sabotage.*

Pour tout incident SSI, voir la Fiche Conseil n°4.

- Protection des systèmes de sécurité-sûreté
  - *exemples de protections techniques : gaines spéciales, autonomie des systèmes, vérification auprès des SSI de la sécurité et de l'inviolabilité des badges et, pour l'informatique, des antivirus…*

Alerte

Décrire le fonctionnement des systèmes d'alerte (hors situation de crise locale et SSE, abordées au chapitre suivant), en distinguant :

- les systèmes internes à l'établissement
  - *moyens d'alerte : téléphone, radio portative, PTI, interphone, réseaux spécialisés, sirènes… ou tout autre dispositif différent de ceux concourant à l'alerte incendie ;*
  - *indiquer la chaîne d'alerte sur site (hors astreinte, traitée ci-après).*

- Consignes en cas d'alerte
  - *consignes générales et dispositifs spécifiques selon les catégories de personnels ou d'emplois (ex. mise en sécurité).*

- Systèmes d'astreinte et de permanence
  - *organisation de l'astreinte (fonctions participantes, régime, moyens à disposition) ;*
  - *modalités de déclenchement de l'astreinte.*

- Les systèmes externes à l'établissement
  - *réseau téléphonique public : préfecture, ARS, brigade de gendarmerie, commissariat de police, pompiers) ;*
  - *éventuellement les liaisons d'alertes spécialisées avec les forces de sécurité intérieure.*

Un exemple de trame d'alerte est disponible à la Fiche Conseil n°1.

Dispositions concernant le personnel et consignes de sûreté

- Procédures de recrutement et d'accès des personnes
  - *pour ces fonctions sensibles, contrôle à l'embauche des personnes en fonction de leur statut :*
    - *agents privés de sûreté (internes ou prestataires) : carte professionnelle délivrée par le CNAPS,*
    - *agents de la fonction publique (titulaires ou non titulaires) : extrait B2 du casier judiciaire[9] ;*
  - *signalement possible sur la base de la convention Santé-Sécurité-Justice entre l'établissement et les services de l'Etat, si cette disposition est prévue.*

- Relation avec les sous-traitants
  - *porter une attention particulière aux entreprises de sous-traitance en veillant à inclure des clauses contractuelles liées à la sécurité : restrictions d'accès, accompagnement de certains sous-traitants dans certaines zones, règles de confidentialité, respect du règlement intérieur….*

- Équipes de protection et de gardiennage
  Personnel : effectif, provenance, formations.
  - *respect et contrôle régulier des règles spécifiques aux sociétés de sécurité (autorisation administrative, formation initiale et continue des agents (CQP-APS[10], sensibilisation la menace terroriste, etc.), conditions d'emploi des chiens de défense…) ;*
  - *insertion dans les marchés publics de sous-traitance d'une ou plusieurs clauses relatives à la détention de qualifications professionnelles propres à chaque métier exercé et contrôle de cette spécificité ;*
  - *organisation du gardiennage, postes tenus, rondes, moyens complémentaires.*

- Rôle éventuel du personnel des autres branches de la sécurité
  - *emploi des équipes de sécurité incendie pour des missions de sûreté, dans le respect de la réglementation applicable[11] ;*
  - *rôle de certaines catégories de personnel lié à leur emploi (personnels soignants) ou lié à une fonction spécifique (guides et serre-files, responsable d'évacuation…).*

- Tests et maintenance périodiques du matériel et du personnel de protection
  - *maintien en condition opérationnelle des équipes de sûreté ;*
  - *maintenance et entretien des équipements de sûreté.*

---

[9] L'article 5 de la loi 83-634 dispose que "nul ne peut avoir la qualité de fonctionnaire … si les mentions portées au bulletin n° 2 de son casier judiciaire sont incompatibles avec l'exercice des fonctions". Cette formulation est reprise à l'article 2 du décret n° 88-145 du 15 février 1988 pour les agents non titulaires.
En cas de renouvellement de contrat, ce bulletin n° 2 doit être à nouveau demandé.
Les mentions éventuelles sur ce bulletin n° 2 doivent être jugées compatibles avec les fonctions à exercer. Cette appréciation relève du pouvoir de l'autorité d'emploi.
Ce document est délivré uniquement à l'administration qui procède au recrutement. Il doit être demandé auprès des services du Casier Judiciaire National (Casier Judiciaire National - Internet B2 -44079 NANTES CEDEX 1 ou cjn2@justice.gouv.fr)

[10] Certificat de qualification professionnelle – agent de prévention et de sécurité.

[11] Se référer à la circulaire du12 août 2015 portant sur l'exercice des activités de sécurité privée et de sécurité incendie par des agents doublement qualifiés (http://circulaire.legifrance.gouv.fr/pdf/2015/08/cir_39950.pdf).

Exemples de mesures de protection, préconisations, adaptables aux risques identifiés

- ***Espaces périphériques[12] et périmétriques :***
  - *limite marquée de la propriété de l'hôpital, état de la clôture du site ;*
  - *limitation/réduction du nombre d'accès envisagée/possible, fermetures de nuit*
  - *affichages dissuasifs (site gardienné, site vidéoprotégé) ;*
  - *entretien et éclairage des zones extérieures en particulier de stationnement et de cheminement piéton ;*
  - *visibilité des espaces extérieurs, clarté de la signalétique, empêcher toute végétation trop haute ou non entretenue ;*
  - *prise en compte de l'exploitation et de la maintenance des dispositifs de filtrage, de contrôle d'accès et de vidéoprotection.*

- ***Alerte :***
  - *préparation d'un annuaire d'urgence (direction, astreinte, services des forces de sécurité intérieure, sapeurs-pompiers, ARS, préfecture, autres services publics, prestataires de première urgence, etc.) ;*
  - *définition des modalités d'alerte (équipement dédié, catégories de personnes désignées, échanges préalables avec les forces locales).*

- ***Accès bâtimentaires / gestion des flux :***
  - *généralisation de l'utilisation d'un badge d'accès, ce dernier pouvant être unique pour plusieurs fonctionnalités (identification du porteur avec photo, gestion des paiements de restauration, des horaires de présence, de l'habillement pour le personnel soignant…) ;*
  - *définition des zones d'accès par type de flux (personnel, patients, familles, prestataires, etc.) :*
  - *dissociation des points d'entrées/sorties du personnel et du public ;*
  - *restriction du nombre de points d'entrées/sorties du site ;*
  - *présence de personnels de sécurité aux points d'entrées/sorties :*
  - *vérification de l'identité des personnes entrantes ;*
  - *contrôle visuel des bagages ;*
  - *contrôle visuel du contenu des véhicules (coffres, intérieur des véhicules, etc.) ;*
  - *détermination des moyens d'accès aux différents parkings, d'identification des véhicules autorisés à accéder au parking personnel ;*
  - *restriction de la liberté de circulation des certaines catégories de patients (dispositif anti-enlèvement de nourrisson, système anti-errance de personnes désorientées).*
  - *restriction des accès aux zones de soins aux seuls patients ;*
  - *circuits spécifiques d'accueil et de sécurisation des détenus, des transports de fonds, des sources radioactives, etc. ;*
  - *accès aux bâtiments non possible depuis les fenêtres du rez-de-chaussée*

[12] L'espace périphérique ne relève pas de la domanialité de l'établissement (voie publique et autre) ce qui nécessite de développer un partenariat avec les communes et propriétaires voisins.

(barreaudage, blocage des fenêtres hors activité…) ;

- *attribution d'un dispositif PTI pour les agents isolés, de sécurité et d'intervention ;*
- *séparation accès livraisons, accès personnels ;*
- *systèmes de filtrage, SAS et contrôle d'accès ;*
- *supervision des contrôles d'accès (délais, alertes…) ;*
- *vidéoprotection des abords (qualité des enregistrements, délai conservation…) ;*
- *configuration des accueils (distance/protections) ;*
- *protection des éléments susceptibles d'être utilisés à des fins malveillantes (pierres, éléments métalliques, etc.) ;*
- *révision et adaptation de la signalétique interne à l'établissement.*

- ***Renforcement des mesures de sûreté dans les volumes intérieurs et des points névralgiques :***
  - *protection et résistance de tous les ouvrants (portes, fenêtres, limiteur d'ouverture) ;*
  - *amélioration/généralisation du niveau global de verrouillage (en respectant des réglementations contre les risques d'incendie et de panique[13]) (clé/cylindre européen standard, clé hors organigramme, un ou trois points etc.) ;*
  - *possibilités de fermeture (confinement) au sein d'un secteur ;*
  - *systèmes de filtrage, SAS de sécurité ;*
  - *supervision des contrôles d'accès (délais, alertes…) ;*
  - *vidéoprotection (qualité des enregistrements, délai conservation…) ;*
  - *détection intrusion (à l'ouverture, volumétrique etc.) / conditions d'intervention ;*
  - *espace dédié aux forces de sécurité pour les conduites de détenus, GAV... (hors de la présence du public, mobilier fixé au sol, pas de fenêtres ou barreaudées, caméra orientée sur la porte d'accès) ;*
  - *inventaire régulier et mis à jour des matériels onéreux et les équiper de puces RFID ou de numéros de série gravés ;*
  - *issues de secours : souvent détournées de leur usage (ex : les personnels fumeurs) feront l'objet d'une attention particulière avec une mise sous UGIS (unité de gestion des issues de secours) préconisée. Leur état et fermeture sera vérifié quotidiennement (ronde). Doter certaines portes de poignées extérieures afin de faciliter une éventuelle intervention des forces de l'ordre.*

[13] Les réglementations dépendent du classement de l'établissement. Les principaux textes régissant ces réglementations sont :

- l'arrêté du 25 juin 1980 portant approbation des dispositions générales du règlement de sécurité contre les risques d'incendie et de panique dans les établissements recevant du public (ERP) ;
- l'arrêté du 10 décembre 2004 portant approbation de diverses dispositions complétant et modifiant le règlement de sécurité contre les risques d'incendie et de panique dans les établissements recevant du public (ERP type U) ;
- les arrêtés du 18 octobre 1977 ou du 30 décembre 2011 portant règlement de sécurité pour la construction des immeubles de grande hauteur et leur protection contre les risques d'incendie et de panique.

- ***Mesures de sécurisation des systèmes d'information :***

L'analyse de risque devra identifier et prioriser les mesures liées à la protection des systèmes d'information. Avec des systèmes de plus en plus ouverts et interconnectés, une vigilance particulière devra être portée sur :

- *les dispositions spécifiques pour prévenir les risques de piratage de tout ou partie des systèmes d'informations, en particulier ceux liés aux matériels biomédicaux, au contrôle d'accès, à la gestion technique centralisée (GTC) et à la gestion technique de bâtiment (GTB) ;*

- *les dispositions permettant de prévenir les risques liés à la perte du patrimoine informationnel de l'établissement notamment par la destruction physique ou logique des actifs indispensables à l'organisme (ex : gestion des flux médicaux) et au bon accomplissement de ses missions (ex : systèmes d'information hospitalier, infrastructures informatiques et de communication, biomédical, gestion technique centralisée.*

En matière de sécurité des systèmes d'information (SSI), l'ensemble des systèmes d'information et de communication (SIC) concourant au bon fonctionnement de l'établissement doivent être pris en considération :

- *systèmes d'information hospitaliers ;*
- *systèmes d'information embarquée ou associée aux dispositifs médicaux ;*
- *informatique générale ;*
- *systèmes de communication ;*
- *gestion technique centralisée ;*
- *les accès au réseau, en interne ou depuis l'extérieur, par les prestataires, les privilèges de connexion accordés.*

Une attention particulière doit être portée sur les interventions réalisées par les tiers. Il convient de veiller en matière de droits sur les systèmes d'information au respect du moindre privilège (Cf. politique de sécurité des systèmes d'information pour les ministères chargés des affaires sociales[14]).

[14] Téléchargeable sur le site internet légifrance : https://www.legifrance.gouv.fr/eli/arrete/2015/10/1/AFSZ1523362A/jo/texte

CHAPITRE III – SÉCURISATION COMPLÉMENTAIRE EN SITUATION D'ATTENTAT OU DE CRISE LOCALE

*La sécurisation de l'établissement en gestion de crise traite des **mesures particulières et immédiates** de sécurité à mettre en œuvre notamment en cas de survenance d'un attentat au niveau local et de risques potentiels de sur-attentat pour l'établissement.*

Toutes les mesures décrites dans ce cadre doivent pouvoir être mises en œuvre sans délai.
Il appartient au directeur (ou à son représentant) de déclencher cette posture réflexe dès qu'il a connaissance d'un événement grave, à l'intérieur ou à proximité de son établissement.
Dans un second temps et après contact auprès de la préfecture et des FSI, le directeur de l'établissement pourra adapter ses mesures de sécurité.

***La préparation de cette situation particulière** nécessitant le **renforcement des mesures de sûreté en vigueur** et/ou la mise en œuvre de mesures supplémentaires – **doit être anticipé en lien étroit avec les services préfectoraux et les forces locales de sécurité intérieure** – afin de :*

- *s'assurer de la prise en charge éventuelle d'un nombre important de victimes dans le cadre du dispositif ORSAN ;*
- *garantir le bon déroulement des soins ;*
- *prévenir le risque de sur-attentat visant l'établissement ou à proximité de ce dernier.*

1. Alerte, communication et information

Il s'agit de préciser dans cette partie le dispositif d'alerte (les moyens d'alerte) et surtout la chaîne d'alerte (qui donne l'alerte) en cas d'événement majeur, afin de s'assurer que les mesures immédiates de sauvegarde (décrites au point suivant) sont bien prises.

- Dossier d'intervention

Réalisation d'un dossier d'intervention pour une force d'intervention du ministère de l'intérieur (voir l'Annexe n°3). Ce dossier doit être validé par les FSI compétentes avant diffusion d'une version finale.

- Schémas d'alerte (interne et externe) et cellule de crise *(qui sont à mettre en œuvre prioritairement)*

***Lors d'une situation de crise (SSE ou autre), il est nécessaire de communiquer rapidement à la fois auprès des FSI, des personnels de l'établissement et de l'ARS**. Cette communication a pour but :*

- *d'adopter immédiatement une posture de sécurisation pour protéger l'établissement ;*
- *d'avertir du passage d'une situation normale à une situation exceptionnelle, tout en rappelant les consignes propres à cette situation de crise ;*
- *d'activer sans délai une cellule de crise pour coordonner les missions à accomplir (communication, suivi de la situation et anticipation, décision) ;*
- *dans un second temps, de pouvoir expliquer aux personnels, aux patients, aux visiteurs, aux sous-traitants et aux fournisseurs les nouvelles contraintes auxquelles ils devront temporairement se soumettre ;*
- *à la fin de la situation de crise et en lien avec la préfecture, les FSI, le parquet et l'ARS ; pouvoir communiquer sur un retour à une situation normale.*

Indiquer qui est en charge des alertes, à partir de quels motifs et avec quels moyens.

Exemples de mesures :

- ***l'alerte :***

  - *alerter selon une trame prédéfinie les forces locales de sécurité intérieure (police ou gendarmerie). Exemple disponible à la Fiche Conseil n°1 ;*
  - *disposer d'un outil complémentaire pour réaliser cette alerte (un système d'alerte d'urgence tel que le système RAMSES sur les secteurs de compétence PN) ;*
  - *mettre en œuvre un outil spécifique pour réaliser l'alerte interne (telles que les applications professionnelles pour smartphone conseillées par l'ANSSI…) ;*
  - *mettre en place un plan de rappel pour les personnels soignants ;*
  - *a contrario, en cas d'attaque terroriste dans l'établissement, diffuser une alarme (différente de celles dédiées à la sécurité incendie) incitant le personnel à se confiner, à évacuer ou à ne pas entrer sur le site.*

- ***la cellule de crise :***

  - *identifier des ressources (salles et équipements) préalablement affectés à la cellule de crise ;*
  - *élaborer et tester les procédures et les moyens de mobilisation de la cellule de crise : qui déclenche, avec quels moyens, pour quel motif, trame de convocation ;*
  - *utiliser un annuaire d'urgence pour joindre les personnels d'astreinte composant la cellule de crise ;*
  - *définir le rôle de chacun sous la forme de fiches réflexes (directeur de crise, synthèse, sécurité-sûreté, communication, RH, finances, pôles de santé, soutien et appui logistique) ;*
  - *fixer des règles de confidentialité et de diffusion de l'information ;*
  - *disposer d'une main courante ou d'un tableau de bord permettant d'assurer le suivi de la situation ;*
  - *effectuer des points de situations régulièrement ;*
  - *prévoir un roulement des équipes participant à la cellule de crise et aménager un espace de repos dans les locaux dédiés à la cellule de crise.*

2. Renforcement de la sécurisation périmétrique et des accès

Décrire les mesures graduelles pouvant être mises en œuvre pour assurer la sécurisation de tous en situation de crise. Il n'y a pas de formalisme pour cette partie, puisque les mesures à prendre ne sont pas toutes transposables d'un établissement à l'autre. Cependant, des pistes de réflexion sont proposées ci-après.

- Mesures existantes renforcées

Un effort particulier devra être porté sur le renforcement de la sécurisation périmétrique et des accès[15].

- Mesures nouvelles

Ces mesures viennent complétées les mesures existantes, renforcées ou non. Elles assurent la cohérence globale du dispositif de sécurisation de l'ES dans des situations extrêmes.

- Mesures souhaitées de la part des FSI

Ces mesures sont à définir en amont avec les FSI. Elles ne peuvent être garanties car elles sont soumises au contexte de la crise et à la disponibilité des FSI.

Exemples de mesures :

- *fermer partiellement ou totalement les accès de l'établissement à titre de précaution. Sous le contrôle d'agents de sécurité ou des agents des FSI, seuls les patients et les ambulances à destination des soins urgents seraient autorisés à entrer sur le site, ainsi que les personnels rappelés*[16] *;*
- *instaurer un périmètre de sécurisation par filtrage des accès aux points névralgiques de l'établissement (SAMU, services des urgences, pharmacies, etc.) ;*
- *déployer des équipements de détection sur les accès publics de certaines zones*[17] *;*
- *gérer les flux afin d'éviter un attroupement excessif aux portes ou un blocage des ambulances sur le site des urgences ;*
- *identifier les itinéraires d'évacuation utilisables pour les personnes mobiles en cas d'attaque terroriste dans l'enceinte de l'ES et définir les modalités d'emprunt ;*
- *identifier les espaces et locaux permettant un confinement des patients et du personnel (pour les personnes non déplaçables) en cas d'attaque terroriste dans l'enceinte de l'ES. Ce zonage ne peut faire l'objet que d'une signalétique discrète ;*
- *disposer de la possibilité d'un report des images de vidéoprotection dans un site externalisé (société privée de télésurveillance, poste de police municipale, PN ou GN) et de couper à distance des flux et des contrôle d'accès en cas de compromission du PCS ;*
- *mettre en place de mesures de protection anti-NRBCe en cas de diffusion d'agents contaminant à l'extérieur ;*
- *mettre en alerte des personnels en charge des SI (renforcement de la surveillance, restriction ou fermeture préventive de certaines connexions, pré-activation du plan de continuité informatique…).*

[15] Action à réaliser en lien avec le chef du pôle des urgences et le directeur du SAMU pour les ES qui en disposent.
[16] Nécessité pour le personnel de l'établissement de disposer d'une carte professionnelle pour faciliter le filtrage.
[17] Par exemple : un portique de détection de masse métallique, scanner à rayon X, magnétomètre.

CHAPITRE IV – MAINTIEN EN CONDITIONS OPÉRATIONNELLES DU PSE ET ARTICULATION AVEC LES AUTRES PLANS

1. Exercices

- Organisation retenue (fréquence et modalités)

La réalisation d'exercices annuels de réaction à une attaque terroriste ou à une situation de sur-attentat doit être effectuée afin de tester les procédures mises en place conformément à l'instruction ministérielle du 16 novembre 2016 relative aux mesures de sécurisation dans les établissements de santé (annexe 1.3).
Ainsi, le PSE et les procédures de réaction du site font l'objet de mises-à-jour périodiques, notamment à la suite des enseignements tirés des exercices. Ces retours d'expérience doivent pouvoir être partagés au niveau régional et local, en lien avec l'ARS et son groupe d'appui technique.

Il est conseillé de faire au minimum un exercice par an

La réalisation d'exercices annuels de réaction à une attaque terroriste ou à une situation de sur-attentat peut prendre plusieurs formes :

- *rappel simple des procédures et du rôle de chacun par le responsable du site ou son chargé de sûreté ;*
- *exercice « sur table » au cours duquel, dans une salle, les employés présentent la réaction qu'ils auraient en cas d'attaque. Celle-ci doit être scénarisée (lieu, nombre et type d'armes des assaillants identifiés) ;*
- *essai des systèmes d'alerte et d'alarmes (plusieurs tests annuels sont conseillés) ;*
- *organisation de reconnaissances exploratoires (lieux d'évacuation, salles de confinement, etc.) ;*
- *exercice de mise en situation avec des personnes simulant l'intrusion[18] (les employés doivent être prévenus de la réalisation de l'exercice mais pas nécessairement de sa date exacte pour éviter des phénomènes de panique). La police ou la gendarmerie sont invités à apporter leur expertise. Ce type d'exercice doit être planifié et préparé en lien étroit avec les préfectures et les responsables des services locaux de sécurité concernés.*

2. Mise à jour du PSE et des procédures

Indiquer la date de la dernière version du PSE.
Une révision annuelle doit être réalisée pour assurer la mise à jour le PSE.
Peuvent être indiqués en plus de la date de la dernière version les changements notables entre la version actuelle et la précédente version.

Le contenu du PSE et en particulier ses fiches réflexes doivent faire l'objet de mises à jour périodiques, notamment à la suite des enseignements tirés des exercices.
Ces mises à jour peuvent utiliser les règles de gestion documentaire de l'établissement.

[18] L'utilisation d'armes, même fictives, est formellement à proscrire dans le cadre de ces exercices.

3. Articulation avec les autres plans

- Plan Vigipirate

Décliner et adapter dans le PSE les mesures sectorielles et les mesures transverses du plan VIGIPIRATE qui sont applicables et que l'établissement est susceptible de mettre en œuvre pour atteindre ses objectifs de sécurité.
Le PSE permet une forte collaboration entre l'établissement de santé et l'ensemble des autorités de l'Etat au niveau local (ARS, préfectures, forces de police et de gendarmerie, etc.).

- Plan blanc

Le PSE doit être intégré dans le plan blanc de l'établissement de santé conformément au décret n° 2016-1327 du 6 octobre 2016 relatif à l'organisation de la réponse du système de santé (dispositif « ORSAN ») et au réseau national des cellules d'urgence médico-psychologique pour la gestion des situations sanitaires exceptionnelles (sous-section 4)[19].

- Plan de continuité d'activité (PCA)

Le plan de continuité d'activité (PCA) doit permettre à l'établissement de continuer à fonctionner en mode dégradé en période de crise ou de perturbation grave et prolongée, en continuant à assurer ses missions essentielles tout en protégeant les patients et les personnels, puis de reprendre progressivement l'ensemble de ses activités normales. Les préconisations de ce plan restent bien évidemment tributaires des mesures générales qui sont prises au niveau national, régional ou local (fermeture éventuelle des haltes garderies, des crèches, des écoles, restrictions de circulation dans les transports en commun et routiers, perturbations du courrier) et de l'évolution de la situation.

Le PCA d'un établissement de santé doit au moins contenir l'exposé de la stratégie de continuité et de reprise d'activité dans l'établissement, selon les types de crises, ainsi que des fiches réflexes précisant, notamment pour l'administration et les services techniques, la conduite à tenir en cas d'évènement imprévu et grave (pannes d'équipements, de serveurs, de routeurs, d'ordinateurs ou de logiciels, coupures de flux d'énergie ou de fluides, évènements météorologiques sérieux…). Pour mieux comprendre la philosophie générale des PCA et se faire une idée des méthodes d'élaboration d'un PCA, on pourra se reporter au guide méthodologique proposé par le secrétariat général de la défense et de la sécurité nationale (SGDSN) intitulé Guide pour réaliser un plan de continuité d'activité. Ce document est disponible sur le site internet www.sgdsn.gouv.fr.

[19] https://www.legifrance.gouv.fr/eli/decret/2016/10/6/AFSP1617819D/jo/texte

3. Annexes

ANNEXE N°1 **PREMIÈRES ACTIONS À CONDUIRE PAR LE DIRECTEUR DE L'ÉTABLISSEMENT**

ANNEXE N°2 **EXEMPLES DE MENACES SUSCEPTIBLES DE SE PRODUIRE DANS UN ÉTABLISSEMENT DE SANTE**

ANNEXE N°3 **TRAME DOSSIER D'INTERVENTION**

ANNEXE N°4 **LISTE DES FICHES MESURES SPÉCIFIQUES VIGIPIRATE À PRENDRE EN COMPTE DANS LES ÉTABISSEMENT DE SANTÉ**

ANNEXE N°1

PREMIÈRES ACTIONS À CONDUIRE PAR LE DIRECTEUR DE L'ÉTABLISSEMENT

1. CONSTITUER UNE EQUIPE PROJET

Afin de mettre en œuvre efficacement le plan de sécurisation de son établissement, le directeur constituera une équipe projet. Le dimensionnement de cette équipe est fonction de la taille et des activités de l'établissement. Elle peut comprendre les fonctions suivantes :

- Directeur adjoint ;
- Responsable « sécurité – sûreté » ;
- Ingénieur qualité ;
- DSI ;
- DRH ;
- Responsable « immobilier – maintenance ».

2. FAIRE UN ÉTAT DES LIEUX DES MESURES EXISTANTES AU SEIN DE L'ES

Afin de capitaliser sur les actions déjà réalisées, le directeur de l'ES recherchera l'existence et s'appuiera sur les travaux suivants :

- un diagnostic sécurité – sûreté (physique et/ou logique) ;
- un plan de protection ;
- la déclinaison des mesures Vigipirate en vigueur ;
- le PCA ;
- le Plan Blanc.

3. IDENTIFIER LES CORRESPONDANTS ET PRENDRE CONTACT AVEC EUX

L'identification et l'activation d'un réseau de correspondants est un atout essentiel à toutes les phases de l'élaboration du plan de sécurisation de l'établissement. Dans cet objectif, le directeur d'établissement prendra contact avec les services suivants :

- l'ARS ;
- la préfecture ;
- les différents correspondants des FSI (en zone Police et/ou Gendarmerie) ;
- le ou les élus en charge de la sécurité et la sûreté dans la commune d'implantation de l'ES ;
- le procureur de la République près le Tribunal de grande instance territorialement compétent.

ANNEXE N°2

EXEMPLES DE MENACES SUSCEPTIBLES DE SE PRODUIRE DANS UN ÉTABLISSEMENT DE SANTÉ

(liste non exhaustive, en complément des menaces propres à l'établissement)

1- Vols sans effraction, dégradations légères, dégradations de véhicules sur parking intérieur de l'établissement.
2- Vols avec effraction (équipements médicaux onéreux, etc.).
3- Dégradations lourdes ou destruction de matériel de valeur (médical, informatique, imagerie médicale…) ex. (razzia dans le hall d'accueil…), dégradations par incendie volontaire (locaux, véhicules sur parking intérieur de l'établissement). Sabotage par un agent ou un prestataire.
4- Injures, insultes et provocations sans menaces, chahuts, occupations des locaux, nuisances, salissures, bousculades.
5- Vols à main armée ou en réunion.
6- Menaces d'atteinte à l'intégrité physique ou aux biens de la personne, menaces de mort, menaces avec arme par nature ou par destination (arme à feu, arme blanche, scalpel, rasoir, tout autre objet dangereux).
7- Agressions physiques : violences volontaires (atteinte à l'intégrité physique, ou psychique).
8- Agression sexuelle, viol.
9- Meurtre, actes de tortures ou de barbaries, autres crimes.
10- Attaques par des moyens improvisés tel que des véhicules bélier.
11- Attaques par armes de guerre (fusils d'assaut, grenades, lances roquettes).
12- Dépôt ou utilisation d'engins explosifs artisanaux, industriels ou militaires de conception simple ou élaborée (dans bagages, drones, véhicules…), déclenchement de ceintures explosives par terroristes.
13- Enlèvement (nouveau-né). Séquestration.
14- Prise d'otages dans l'enceinte de l'ES, enlèvement pouvant être suivi d'exécution.
15- Réalisation d'un sur-attentat au sein de l'établissement ou à proximité afin d'empêcher les secours d'intervenir ou de limiter la prise en charge des victimes.
16- Cyber-attaque (perturbation, intrusion, vol d'informations…).
17- Vols d'équipements sensibles ou de produits de santé (dont tenues et contre mesure médicale NRBC-e, si disponibles dans l'établissement).

ANNEXE N°3

TRAME DOSSIER D'INTERVENTION

1. OBJECTIF

Cette trame a pour but de collecter dans un dossier les principales informations fondamentales dont une force d'Intervention du ministère de l'intérieur aura besoin dans le cadre de la gestion d'une crise majeure. Ce dossier confidentiel doit être communiqué au service de police ou de gendarmerie de proximité. Ce document doit être daté. L'idéal est de mettre à jour ce dossier une fois par an.
Il doit impérativement être clair, précis, facile à comprendre et ne pas créer d'ambigüité.

2. GÉNÉRALITÉS

Pour faciliter la lecture et l'emploi du dossier d'intervention, il est demandé de le fournir en **format PDF**. En plus de ce dossier, il est demandé de fournir en format PDF les **plans originaux d'évacuation ou d'intervention** (à privilégier). Ce dossier doit pouvoir être disponible et communicable en permanence.

3. CONTENU

- **généralités sur le site** : nom, adresse, coordonnées GPS, type d'établissement, superficie, nombre de personnes affectés à la sécurité & sûreté, nombre de personnes présentes sur le site, service de police ou gendarmerie territorialement compétent (nom et téléphone), risques particuliers... ;
- **contacts principaux** avec en priorité des numéros **24/7** (directeur de l'établissement, directeur de la sûreté, directeur technique, PC Sûreté, PC Sécurité (incendie)...) ;
- **vue satellite avec les accès renseignés** (piéton, véhicule, issue de secours...) ;
- **plan de type évacuation ou d'intervention** (à privilégier) par niveau {sous-sols, tous les étages, galeries techniques, toitures) avec les accès renseignés (piéton, véhicule, issue de secours, échelle à crinoline...) ;
- **photographies des façades ;**
- emplacement sur un plan du ou des **PC Sécurité et / ou Sûreté** ;
- **système de vidéoprotection :** emplacement de tous les retours vidéos internes ou externes au site, accès possible sur tablette ou Smartphone (adresse IP, port, login et mot de posse), plan d'implantation des caméras, baie technique, lieu d'extraction des images, nœuds de raccordement ;
- **système de détection :** localisation, type, couplage avec le système de vidéoprotection, lieu de gestion ;
- **contrôle d'accès :** localisation, type (badges, clés, biométrie. ouverture commandée...), couplage avec le système de vidéoprotection, lieu de gestion ;
- emplacement sur un plan des **réseaux et des coupures des sources d'énergie** (électricité, gaz) ;
- emplacement sur un plan du ou des **groupe (s) électrogènes)** ;
- emplacement sur un plan des **zones de stockage des produits dangereux** ;
- **informations sur la résistance des matériaux** utilisés pour cloisons intérieures, murs extérieurs, sols, plafonds, portes, serrures... ;
- **moyens d'ouverture de tous les accès** (type "passe général") : qui en détient, emplacement des doubles (renseigné sur un plan).

ANNEXE N°4

LISTE DES FICHES MESURES SPÉCIFIQUES VIGIPIRATE À PRENDRE EN COMPTE DANS LES ÉTABLISSEMENTS DE SANTÉ

La présente liste constitue un ensemble non exhaustif de fiches mesures non protégées pouvant s'appliquer aux établissements.
Les fiches mesures n'ayant pas vocation à être rendues publiques, il est demandé de se rapprocher des correspondants VIGIPIRATE pour obtenir communication de leur contenu détaillé.
Les fiches ont vocation à être mises à jour régulièrement, il est conseillé de vérifier la parution de nouvelles versions de ces documents.

1. Domaine alerte – mobilisation (ALR)

ALR 10-03	Interdire l'usage et/ou le transport des drones civils dans le périmètre déterminé
ALR 10-04	Signaler toute transaction suspecte, vol ou disparition de matières et tout indice d'événement NRBC-e
ALR 11-01	Activer les cellules de veille et d'alerte et les cellules de crise
ALR 20-01	Elaborer et mettre à jour un plan de continuité d'activité (PCA)
ALR 22-07	Déployer des moyens permettant de détecter et de gérer la présence d'explosifs sur les sites

2. Domaine bâtimentaire (BAT)

BAT 12-05	Mettre en œuvre des dispositifs de protection pour faire face aux différents modes opératoires terroristes
BAT 20-01 BAT 21-01 à 23-01	Sûreté des accès des installations
BAT 30-01 BAT 30-02 BAT 31-01	Sûreté interne des installations et bâtiments désignés (complète celle relative à la sûreté des accès)
BAT 32-02	Mettre en œuvre des dispositifs de protection pour faire face aux différents modes opératoires terroristes

3. Domaine de la santé (SAN)

SAN 10-01	Assurer une veille sanitaire permanente visant à détecter au plus tôt un événement ou un attentat NRBC-e insidieux
SAN 10-02	Garantir un niveau minimal de capacité analytique dans le domaine de la qualité de l'eau et des maladies infectieuses et cibler les analyses en fonction de la menace
SAN 20-01	Maintenir une capacité de réponse et d'adaptation de l'offre de soins
SAN 20-02	Maintenir une capacité de reprise et d'adaptation de l'offre de soins
SAN 21-01	Suivi de l'activation des procédures de rappel du personnel et plans blancs par les établissements de santé
SAN 22-02	Activer la réserve sanitaire
SAN 50-01	Protéger les établissements de santé
SAN 52-01	Renforcer les mesures de sécurité des accès aux établissements de santé désignés

4. Fiches Conseil

FICHE CONSEIL N°1 **TRAME DE MESSAGE D'ALERTE**

FICHE CONSEIL N°2 **CONDUITE À TENIR DANS LE CADRE D'UNE ALERTE À LA BOMBE**

FICHE CONSEIL N°3 **DÉCOUVERTE D'UN OBJET OU RÉCEPTION D'UN COLIS SUSPECT**

FICHE CONSEIL N°4 **INCIDENT DE SÉCURITÉ SUR UN POSTE DE TRAVAIL INFORMATIQUE**

FICHE CONSEIL N°5 **LE REPÉRAGE DES CAS DE RADICALISATION**

FICHE CONSEIL N°6 **LE CONTRÔLE ET LA FOUILLE DES BAGAGES ET SACS**

FICHE CONSEIL N°1

TRAME DE MESSAGE D'ALERTE

Pour le contact des forces de sécurité intérieure

En présence d'un événement grave, l'alerte des services de police ou de gendarmerie est réalisée dans les plus brefs délais.

L'alerte est faite par le directeur d'établissement ou un agent formé et désigné par ses soins. Pour cela, l'agent dispose d'un téléphone dédié au _____.

A défaut, tout autre moyen de communication rapide et sûr peut être utilisé.

L'agent :

1. décroche le téléphone et compose le n°**17** ou envoie un SMS au **114** ;
2. dès la liaison établie, suit la **trame du message d'alerte :**

A. **Identification**

Mon nom, ma fonction, je suis à *nom de l'ES,* mon n° de téléphone pour être rappelé est le *: numéro de téléphone.*

B. Type d'événement et risques

Nous sommes en présence d'un :

☐ *agression physique* ☐ *fusillade* ☐ *explosion* ☐ *colis suspect* ☐ *autre (préciser)*

C. Adresse exacte

Nous sommes au *adresse du site.* L'accès des secours se fera par : *adresse et description du point d'accès*

D. Nombre de public (patients et visiteurs) et de personnels sur site

Nous sommes XX personnes, dont XX non autonomes.

Il n'y a pas (ou il y a XX) de blessé ou mort.

E. **Actions effectuées**

☐ *évacuation* ☐ *confinement de patients* ☐ *premiers secours* ☐ *autre (préciser)*

NE PAS RACCROCHER EN PREMIER

Connaître les numéros d'urgence

Les **numéros d'appel d'urgence** permettent de **joindre gratuitement les secours 24h/24**

Service	Numéro à composer	Dans quel cas ?
Numéro d'appel d'urgence européen	112	Si vous êtes victime ou témoin d'un accident dans un pays de l'Union Européenne
Le Service d'aide médical urgente (SAMU)	15	Pour obtenir l'intervention d'une équipe médicale lors d'une situation de détresse vitale, ainsi que pour être redirigé vers un organisme de permanence de soins
Police-Secours	17	Pour signaler une infraction qui nécessite l'intervention immédiate de la police ou de la gendarmerie
Sapeurs-pompiers	18	Pour signaler une situation de péril ou un accident concernant des biens ou des personnes et obtenir leur intervention rapide
Numéro d'urgence pour les personnes sourdes et malentendantes	114	Si vous êtes victime ou témoin d'une situation d'urgence qui nécessite l'intervention des services de secours. Numéro accessible par FAX et SMS

FICHE CONSEIL N°2

CONDUITE À TENIR DANS LE CADRE D'UNE ALERTE À LA BOMBE

SOMMAIRE :

Introduction

Il s'agit des engins explosifs improvisés (E.E.I.) qui ne peuvent pas être découverts, mais qui sont signalés sous le couvert de l'anonymat ou sous une identité empruntée :

- le plus souvent par téléphone ;
- plus rarement par lettre ou message.

Si la plupart du temps, les « alertes à la bombe » se révèlent fausses, il ne faut pas sous-estimer une orchestration pour :

- tester les réactions des équipes de sécurité ;
- évaluer leurs effectifs, leurs moyens ;
- préparer un attentat réel ;
- déclencher des actions de diversion contre les équipes de déminage ;
- se venger et nuire à l'établissement.

PHASE 1 : l'appel anonyme

S'imprégner de la fiche réflexe n°1, afin de recueillir le maximum d'informations pouvant aider à :

- localiser un objet non identifié qui devient ainsi, suspect ;
- définir sa nature, son volume ;
- déterminer son emplacement ;
- connaître l'heure théorique d'explosion.

Les appels anonymes doivent être pris avec sérieux dès leur réception. L'agent du standard est par sa fonction le plus exposé à recevoir ce type d'appel. La qualité du recueil des éléments peut s'avérer déterminante pour la réussite d'une enquête. Il faut avoir à l'esprit le fait que les éléments pourront être exploités notamment en cas de menace avérée.

Principes généraux :

Il est essentiel que la personne recevant l'appel se comporte de la manière suivante :

- rester calme, ne pas paniquer ;
- écouter ;
- traiter cet appel comme tous les autres appels ;
- ne pas interrompre l'appelant, mais ne pas hésiter à lui dire que la ligne est mauvaise pour le faire répéter ; noter précisément le contenu du message transmis.
- noter le numéro ou penser à l'issue de l'appel à le rechercher dans l'historique du téléphone ;
- être attentif à l'environnement sonore qui entoure l'interlocuteur
- tâcher d'obtenir le plus de renseignements possible en se référant au formulaire ci-après (fiche réflexe n°1), compléter si possible le formulaire au fil de l'appel ;
- remplir le formulaire complètement et le remettre au responsable désigné pour la sûreté dans l'établissement.

Il est important d'essayer dans la mesure du possible de prolonger au maximum la conversation pour obtenir le plus d'éléments possibles. Ne pas raccrocher trop vite. Il faut que montrer à l'interlocuteur qu'il est accordé de l'importance au discours qu'il tient. À aucun moment l'interlocuteur ne doit avoir l'impression de répondre à un questionnaire, être subtil dans la façon de recueillir les informations.

RESTER DISCRET À LA SUITE DE CET APPEL ET CE POUR ÉVITER DE CRÉER

UNE PANIQUE OU DE GÊNER LES INVESTIGATIONS ULTÉRIEURES

PHASE 2 : transmission de l'alerte

- rendre compte au responsable du site: directeur, chef de la sécurité et de la sûreté, … qui est seul responsable de l'évacuation ou non de ses locaux ;
- alerter, sans tarder, les services de police ou de gendarmerie (17).

L'intervention du service de déminage est subordonnée à la découverte physique d'un objet ou d'un véhicule suspect (en règle générale, les démineurs ne se déplaceront pas tant que rien n'est trouvé, sauf si la conjoncture laisse penser que l'alerte a de fortes chances d'être réelle).

Toutefois, Le responsable de l'équipe d'intervention prendra contact avec le requérant pour lui donner la marche à suivre et le guider dans les prises de décision qui incombe au chef d'établissement.

PHASE 3 : l'évacuation

Sur ordre du directeur d'établissement, elle sera de :

- 100 mètres à couvert pour un paquet suspect, quel que soit son volume ;
- 200 mètres à couvert pour un véhicule suspect.

Le personnel et les patients sont déplacés de leur service :

- après en avoir examinés le contenu de la pièce ;
- si présents, en emportant leurs effets personnels ;
- en laissant toutes les clefs sur leur serrure ;
- la dernière personne quittant la pièce, le local, le poste, appose une marque apparente signalant qu'aucun objet suspect n'a été découvert ;

- si une personne découvre un objet suspect, elle mémorise son emplacement rend compte et reste à la disposition du responsable du site. Dans ce cas, interrompre toute recherche, terminer rapidement l'évacuation, attendre l'arrivée des démineurs. Ne pas entreprendre d'autres recherches avant que l'objet soit traité et que le doute soit levé.

PHASE 4 : opérations de fouilles et de recherches

Le nombre et La composition des équipes de fouille ne sont pas exhaustifs. Le travail sera confié à du personnel connaissant les lieux, les équipes pourront être renforcées par des policiers, gendarmes, maîtres de chien de recherche d'explosif…

Les opérations doivent être coordonnées depuis un PC situé au périmètre de sécurité : 100 ou 200 mètres.

Appliquer la fiche réflexe n°2. Il est impératif d'indiquer aux personnels affectés à la fouille que leur tâche se limite à chercher et signaler tout objet d'apparence suspecte et qu'ils doivent :

- agir avec précaution ;
- ne pas modifier les conditions ambiantes : allumer ou éteindre un éclairage, un outil informatique, une TV... ;
- repérer les défauts qui semblent récents: élément de faux plafond déplacé, vis de plaque d'aération manquante, visiblement manipulée, extincteur déplombé… ;
- fouiller les locaux techniques, ascenseurs… ;
- ne rien déplacer, n'ouvrir aucun paquet, sac, colis, bagage, ne pas manipuler d'objet qui ne soit pas dument reconnu. Le risque étant de faire fonctionner le piège ou de le rendre dangereux et de compliquer les opérations de déminage ;
- rendre compte précisément de toutes les anomalies rencontrées.

CONDUITE À TENIR DANS LE CADRE D'UNE ALERTE À LA BOMBE

Fiche réflexe n°1

Recueil d'informations sur appel anonyme

Service :
Téléphone :
Nom et qualité de la personne recevant l'appel :
Date et heure d'appel (J/M/A/H) :
Durée de l'appel :

Origine de l'appel :
☐ Interne ☐ Extérieur ☐ Mobile ☐ Inconnu

INSCRIPTION DE L'INTÉGRALITÉ DU MESSAGE RECU :

« Ne jamais interrompre la personne »

Caractéristiques de la personne qui appelle :

Sexe : **Age approximatif :**

Caractéristiques de la voix :		Élocution :		Bruits de fond :	
Forte	Douce	Rapide	Lente	Silence	Vacarme
Aigüe	Grave	Distincte	Indistincte	Voix	Musique
Rauque	Claire	Bégayant	Articulée	Radio	Télévision
Nasillarde	Calme			Enfants	Animaux
Etat d'ivresse	Etouffée			Moteurs	Electroménagers
Déformée					
Accent :		**Attitude :**		**Ambiance de fond :**	
Local	Régional	Revendicative	Ploie	Aéroport	Rue – circulation
Etranger, préciser :		Menaçante	Grossière	Gare	Usine
Sans		Obscène	Irritée	Port	Restaurant – bar
		Incohérente	Hésitante	Stade	Autre lieu public
				Absence de bruit particulier	
Expression :		**Type de message :**		**Autres détails :**	
Courante	Rudimentaire	Enregistré	Lu		
Argotique	Recherchée	Spontané			
Professionnel					

CONDUITE À TENIR DANS LE CADRE D'UNE ALERTE À LA BOMBE

Fiche réflexe n°2

Exécution des opérations de fouille et recherche

Il s'agit de mettre à l'abri les patients, leurs visiteurs et le personnel de l'ES en respectant par défaut les distances suivantes :

Rayon d'évacuation :

EEI[20] : 100 m à couvert ;

Véhicule : 200 m à couvert.

Les FSI et/ou les démineurs peuvent décider à tout moment de modifier les conditions d'évacuation décrites ci-après en fonction de la nature de la menace.

Heure d'explosion / Lieu d'explosion	**DÉTERMINÉE**	**INDÉTERMINÉE**
DÉTERMINÉ	- évacuation immédiate - fouille immédiate de l'endroit désigné - stopper les fouilles **30 mn avant et après** l'heure prévue d'explosion	- évacuation immédiate - fouille immédiate sans interruption dans le temps
INDÉTERMINÉ	- évacuation immédiate ; - fouille immédiate de toute l'installation - stopper les fouilles **30 mn avant et après** l'heure prévue d'explosion	- -pas d'évacuation - -fouille immédiate

Décision d'évacuation :

- directeur de l'établissement ;
- responsable de l'ordre public s'il y a danger imminent ou si la voie publique est concernée.

Modalités d'évacuation pour les personnes évacuées :

1/ Examiner la pièce à évacuer :

- aucun objet suspect ➔ marque sur la porte signalant l'inspection négative ;
- objet suspect ➔ mémoriser l'emplacement et le signaler au responsable des fouilles.
  Accélérer l'évacuation.

2/ Emporter tous les effets personnels (afin de ne pas multiplier le nombre d'objets abandonnés).

[20] Engin Explosif Improvisé: bagage, carton, colis, sac, etc.

FICHE CONSEIL N°3

DÉCOUVERTE D'UN OBJET OU RÉCEPTION D'UN COLIS SUSPECT

SOMMAIRE

Introduction – consignes importantes

En cas de découverte d'un paquet abandonné ou d'un colis suspect, il est important de respecter les consignes suivantes :

- **ne pas manipuler l'objet** : ne pas le déplacer, l'ouvrir, le mouiller, le couvrir ;
- **ne pas utiliser à proximité du colis suspect d'appareils qui émettent des ondes** (téléphone portable, tablette…) ou qui sont connectés (Wifi, Bluetooth) car il existe des systèmes pouvant être activés de cette façon ;
- **ne pas modifier l'environnement des lieux** en allumant ou éteignant la lumière par exemple, ou en faisant fonctionner un appareil électrique ;
- **se tenir à distance**, puis prévenir immédiatement le responsable ou le service de sûreté. Dans le cas où du public (patient ou visiteur) serait présent, l'éloigner dans le calme ;
- **mémoriser visuellement l'objet** afin de pouvoir donner un maximum d'informations aux forces de sécurité intérieure qui interviendront (voir en annexe n°1 la fiche réflexe à cet effet) ;
- **prévenir ou faire prévenir les forces de sécurité intérieure** en composant le **17** depuis un téléphone fixe ;
- dans le cas d'un paquet abandonné, rechercher le propriétaire en diffusant un message sonore.

ATTENTION : ne pas avoir de vue directe sur le colis ou l'objet « suspect ».

Cas n°1 : découverte d'un objet suspect

1. Évacuation

L'alerte signalant l'évacuation peut se faire par haut-parleurs ou par téléphone lorsque le réseau interne permet de faire sonner l'ensemble des postes fixes. **L'utilisation de l'alarme incendie n'est pas recommandée,** car la procédure d'évacuation est différente. En effet, dans le cas d'un colis « suspect », il faut que chacun prenne ses affaires personnelles (mallette, sac à dos…) afin de ne pas multiplier le nombre d'objets abandonnés et donc potentiellement suspects.

- **suivre les instructions** des services de sécurité et de sûreté quant à la mise en sécurité des personnes ;
- **vérifier bien que personne ne reste à l'intérieur des locaux**, fermez la porte (SANS LA VERROUILLER), et inscrivez-y la mention « VIDE » (au marqueur, au feutre ou à la craie).

2. **Regroupement**

- au point de regroupement désigné, effectuer le comptage du personnel et des patients afin de s'assurer de n'avoir oublié personne à l'intérieur de la zone d'exclusion ;
- s'éloigner des surfaces vitrées, afin d'éviter les éclats de verre en cas de déflagration ;
- si les services de police ou de gendarmerie ne sont pas encore sur place, interdire l'accès du bâtiment mis en sécurité.

3. **À l'arrivée des secours**

- les personnes connaissant bien les lieux doivent **signaler auprès des services de secours** (FSI, pompiers) **tout élément susceptible d'entraîner un risque** (exemple : présence d'un de gaz médicaux ou d'une arrivée générale de gaz, entrepôt de produits inflammables dans une pièce…) ;
- **suivre à la lettre les instructions** qui sont données par les services de secours ;
- ne pas retourner dans les locaux qu'après l'autorisation expresse des responsables des services de secours.

4. **Que faire après ?**

L'objet est un bien abandonné qui ne représente pas de danger : profiter de cet incident pour sensibiliser le personnel sur les consignes à respecter lors de la découverte d'un objet suspect.

L'objet contenait un explosif qui ne s'est pas déclenché ou qui a été désamorcé : les forces de sécurité intérieure vont auditionner toutes les personnes susceptibles de fournir un renseignement.

- **sauvegarder vos enregistrements de vidéoprotection** ;
- ne toucher à rien dans les locaux tant que les services chargés de relever les traces et indices ne sont pas intervenus (identité judiciaire) ;

5. **Préconisations**

- prévoir une procédure d'évacuation et sensibiliser le personnel à cette procédure ;
- effectuer régulièrement des exercices et prévoir un affichage de cette procédure dans des lieux réservés aux personnels (non accessibles au public) ;
- avant de rentrer les poubelles, vérifier que les containers soient bien vides ;
- ne jamais laisser sur la voie publique des objets pouvant être dangereux. Par exemple : bonbonnes de gaz, produits nocifs…
- faire en sorte qu'ils ne soient pas laissés sans surveillance jusqu'au passage des encombrants / éboueurs / sociétés spécialisées dans le conditionnement de ce type de produits ;
- en cas de vol de matériaux dangereux (gaz / produits chimiques…) lors d'un transport par exemple, le signaler immédiatement aux services de police ou de gendarmerie avec le contenu et la nature exact du vol ;
- signaler toute « perte » / « vol » dans un inventaire fait au sein de votre établissement avec ce type d'équipement.

Cas n°2 : réception d'un colis ou d'un pli suspect

Deux types d'attaques peuvent coexister : le colis piégé (à l'explosif ou avec une substance dangereuse) et le pli contenant une substance dangereuse.

1. **Les signaux d'alerte :**

- plis épais et rigides, enveloppes renforcées (une enveloppe ordinaire ne peut être que très difficilement piégée – les explosifs et les systèmes de mise à feu nécessitent l'emploi d'enveloppes plus solides) ;
- présence de traces graisseuses sur l'enveloppe ou l'emballage ;
- courrier dont l'origine n'est pas identifiée ou identifiable (expéditeur inconnu du destinataire) ;
- sur-affranchissement par rapport au poids réel (nombreux timbres ayant une valeur élevée) ;
- marqué « fragile » alors que ce n'est pas nécessaire ;
- présence de fils ou de feuilles métalliques si le colis est endommagé ;
- bruits suspects (grésillements…) ;
- le pli / colis a une répartition inégale de son poids ;
- **réception d'un pli / colis par un coursier ;**
    - si le pli / colis a été déposé en l'absence du personnel de la réception ;
    - si le coursier a le visage dissimulé ou casqué et / ou quitte les lieux précipitamment sans explications.

2. **Attaque aux « Enveloppes contaminées »**

Les préconisations ci-dessous sont à mettre en œuvre en gardant à l'esprit qu'elles ont plus vocation à « rassurer » le personnel, si ce dernier craint (par un sentiment d'insécurité) ce type d'attaque.

Si le pli a été ouvert et que l'on découvre une « poudre » à l'intérieur :

- reposer immédiatement la lettre, ne plus la manipuler, ni la toucher, ni la renifler… ;
- si le pli est tombé au sol, le laisser sur place (ne pas le transporter) ;
- ne pas faire de mouvements brusques et ne pas s'épousseter (pour éviter la dispersion du produit) ;
- fermer les ouvertures de la pièce (éviter les courant d'air) – couper la climatisation / ventilation ;
- quitter les lieux dans le calme et fermer la pièce (en apposant une signalétique d'interdiction d'entrer) ;
- les personnes présentes à l'ouverture doivent rester ensemble et se confiner dans un local à proximité en évitant tout contact avec les autres (sans climatisation / aération / ouverture de fenêtre) ;
- dresser une liste des personnes ayant été en contact direct avec la substance, ainsi que celles se trouvant à proximité (mais ne l'ayant ni respiré / touché) ;
- les inviter à se laver soigneusement avec du savon les parties du corps exposées, puis condamner les sanitaires jusqu'à leur nettoyage complet avec désinfectant ;
- éviter tout contact entre les personnes ;
- recueillir pour les services de police ou de gendarmerie une description précise de l'objet incriminé (pli ouvert ou fermé, taille, couleur, timbres, origine, oblitération, circonstance de la découverte, circuit emprunté dans l'établissement…). Se référer à l'annexe 1 ;
- attendre calmement les secours.

3. **Réouverture des locaux**

- **toujours obéir aux instructions des services de secours ;**
- ne pas prendre d'initiative de réouverture ou de pénétration ou sortie des lieux.

DÉCOUVERTE D'UN OBJET OU RÉCEPTION D'UN COLIS SUSPECT

Fiche réflexe n°1

Recueil d'informations sur l'objet suspect

Fiche synthétique destinée à collecter auprès des témoins et/ou des primo-intervenants l'ensemble des informations et actions réalisées jusqu'à l'arrivée des services de déminage.

Ces éventuels examens doivent avoir été effectués avant la découverte du caractère suspect de l'objet et non après !

Cette fiche doit être complétée après avoir décidé des premières réactions immédiates et autres mesures conservatoires (évacuation de la zone, mise en place d'un périmètre de sécurité, etc…).

NE JAMAIS TENTER DE DÉPLACER OU D'OUVRIR LE CONTENANT

1 – CIRCONSTANCES ET LIEU DU SIGNALEMENT

Date et heure : / /20 – : Lieu de découverte :

Localisation exacte : .....

.....

Circonstances de découverte : .....

.....

.....

.....

Provenance si connue (expéditeur, transporteur, destinataire) : .....

.....

.....

.....

Événement enregistré par la vidéoprotection : ☐ OUI ☐ NON Témoins : .....

.....

Position de l'élément dans son environnement : .....

.....

.....

.....

Détails sur l'environnement (volume, encombrement, obstacle) : .....

.....

.....

.....

.....

2 – DESCRIPTION DE L'ÉLÉMENT SUSPECT OU AUTRE SUPPORT

Type : ☐ Pli ☐ Colis ☐ Bagage ☐ Véhicule ☐ Autre : .....

Aspect : ☐ Solide ☐ Liquide ☐ Autre : .....

Format / taille/ poids (si connu avant) : .....

.....

.....

.....

.....

Détails des différents composants visibles : .....

.....

.....

.....

.....

Couleur : .....

.....

Odeur particulière : ☐ NON ☐ OUI : .....

.....

Description complémentaire : .....

.....

.....

.....

.....

.....

.....

3 – CHRONOLOGIE ET ACTIONS RÉALISÉES

Heure Alerte interne : ..... **Heure Alerte FSI :** .....

Heure Alerte Déminage : .....

Examen visuel (ne jamais ouvrir l'élément) : ☐ NON ☐ OUI, Résultats : .....

.....

.....

.....

Examen Rayons X : ☐ NON ☐ OUI, Résultats : .....

.....

.....

Autre(s) information(s) : .....

.....

.....

Périmètre de sécurité : ☐ NON ☐ OUI, détails de la zone d'exclusion : .....

.....

.....

Ligne guide pour artificiers : ☐ NON☐ OUI Prises de photos / vidéos : ☐ NON☐ OUI

FICHE CONSEIL N°4

INCIDENT DE SÉCURITÉ SUR UN POSTE DE TRAVAIL INFORMATIQUE

1. Maintenir la machine allumée et la déconnecter du réseau

Surtout maintenez la machine compromise sous tension et ne la redémarrez pas, car il serait alors impossible de connaître les processus qui étaient actifs au moment de l'intrusion. Vous risqueriez de provoquer une modification sur le système de fichiers et de perdre de l'information utile pour l'analyse de l'attaque

Puis, déconnecter-la du réseau. Cela permet de stopper l'attaque si elle est toujours en cours. S'il était toujours connecté à la machine, l'intrus n'aurait plus de contrôle sur celle-ci et ne pourrait donc pas surveiller ce que vous faites et/ou modifier des fichiers.

2. Prévenir le responsable de la sécurité des systèmes d'information (RSSI)

Prévenez immédiatement le RSSI (ou votre correspondant informatique habituel, selon la procédure en vigueur) et votre hiérarchie qu'une intrusion a été détectée.

La procédure d'alerte doit être documentée et connue des utilisateurs.

Des recommandations techniques à destination des intervenants techniques sont indiquées sur le site de l'ANSSI. Un formulaire type de déclaration d'incidents est proposé dans la PSSI-MCAS[21].

[21] Téléchargeable sur le site internet légifrance :
https://www.legifrance.gouv.fr/eli/arrete/2015/10/1/AFSZ1523362A/jo/texte

FICHE CONSEIL N°5

LE RÉPERAGE DES CAS DE RADICALISATION

Ce repérage répond à une double nécessité pour l'administration de l'établissement : être alertée dès les premiers signaux faibles afin de prévenir la radicalisation, et être en appui de la chaîne hiérarchique face à ce phénomène.

C'est donc au management de proximité de détecter tous les signaux faibles d'un début de radicalisation : cadre de santé, chef de service, etc.

La radicalisation n'a pas de définition juridique mais pratique, c'est la définition interministérielle émanant du secrétariat général du comité interministériel de prévention de la délinquance et de la radicalisation (SG/CIPDR): « *Par radicalisation, on entend le processus par lequel un individu ou un groupe adopte une forme violente d'action, directement liée à une idéologie extrémiste à contenu politique, social ou religieux qui conteste l'ordre établi sur le plan politique, social ou culturel* ».
Cette définition prend en compte toutes les formes de radicalisation et ne se limite pas à la radicalisation islamiste.
La radicalisation présente ainsi deux caractéristiques majeures :

- elle n'est caractérisée que lorsqu'il y a violence (physique, verbale ou morale) ;
- elle repose sur une série d'indicateurs cumulatifs, téléchargeables sur le site internet du ministère de l'Intérieur[22].

Le directeur de l'établissement peut décider du signalement d'un cas de radicalisation supposé auprès du centre national d'assistance et de prévention de la radicalisation dont le numéro vert est :

0 800 00 56 96

S'agissant des manquements à l'obligation de neutralité, au principe de laïcité et à l'obligation de réserve, les exemples suivants peuvent être donnés, qui doivent alerter l'encadrement :

- le prosélytisme : chercher à promouvoir une religion dans son environnement professionnel ;
- le port d'un signe religieux ostentatoire sur le lieu de travail et durant le temps de travail ;
- le refus de serrer la main, d'être reçu par une personne de l'autre sexe, ou d'être placé sous l'autorité hiérarchique d'une femme ;
- l'utilisation de locaux affectés à l'hygiène, au repos et à la restauration pour exercer une pratique religieuse ;
- une prière dans un local d'entreposage de matériel.

À ce stade, il appartient au cadre de proximité de faire remonter l'information de manière strictement confidentielle à la chaîne hiérarchique.

[22] Le référentiel et le tableau de synthèse des indicateurs de basculement sur le site du SG/CIPDR : http://www.interieur.gouv.fr/SG-CIPDR/Prevenir-la-radicalisation/Prevenir-la-radicalisation

FICHE CONSEIL N°6

LE CONTRÔLE ET LA FOUILLE DES BAGAGES ET SACS

Policiers et gendarmes

Les policiers et les gendarmes sont habilités à effectuer des ouvertures et fouilles de sacs (selon les conditions fixées par le code de procédure pénale).

Agents de sécurité privée[23]

Dans le cadre du contrôle d'accès des ES, les agents de sécurité privée, s'ils sont spécialement habilités par l'autorité préfectorale à la fouille, peuvent effectuer des opérations de contrôle :

- faire des palpations de sécurité (c'est-à-dire passer les mains sur les habits d'une personne pour s'assurer qu'elle ne porte pas une arme) ;
- se faire ouvrir et regarder à l'intérieur d'un sac sans le fouiller.

Dans tous les autres cas il faut l'assentiment express de la personne.

Ces mesures, prévues par le code de la sécurité intérieure (**art. L613-2**), sont appliquées en cas de circonstances particulières et motivées par arrêté du préfet. **Elles sont soumises au consentement de la personne contrôlée. Le refus de se soumettre à ce contrôle peut justifier l'interdiction d'accès au site et/ou l'appel éventuel aux FSI. L'interdiction d'accès doit être prévue dans un règlement intérieur et être clairement affichée à l'entrée du site.** En cas de difficultés, il pourra faire appel aux FSI.

Quel motif à fouiller les sacs à l'entrée d'établissements de santé ?

L'inspection visuelle des sacs à l'entrée de certains lieux publics vise à empêcher l'introduction d'objets ou de substances dangereuses qui permettraient la commission d'actes terroristes.
La loi n'autorise les agents de sécurité privée qu'à opérer une inspection visuelle des sacs de voyage. Des lieux recevant du public et à forte affluence ont déjà été la cible d'attentats. Une vigilance particulière est donc nécessaire.
Le refus de se soumettre à ce contrôle peut justifier l'interdiction d'accéder au site.

Peut-on refuser l'accès à certains lieux ?

Oui en certaines circonstances et pour certains lieux. Les mesures de sécurité peuvent être renforcées et l'accès refusé pour les personnes non habilitées ou ne satisfaisant pas aux exigences des mesures de contrôle. Par exemple le règlement intérieur, affiché à l'entrée d'un établissement, peut prévoir l'interdiction d'accès à une personne refusant de se soumettre aux mesures de sûreté exigées.

[23] L'agent doit être titulaire d'un certificat de qualification professionnelle (CQP-APS) et d'une carte professionnelle délivrée par le CNAPS. Voir guide ONVS.

5. Textes de référence

Pour accompagner l'établissement dans la rédaction de son PSE, il dispose des documents suivants :

- **Ministères sociaux**

- *Instruction n° SG/HFDS/2016/340 du 16 novembre 2016 relative aux mesures de sécurisation dans les établissements de santé ;*
- *Guides « Vigilance attentats : les bons réflexes » à destination des équipes de direction et du personnel des établissements de santé, sociaux et médicaux sociaux ;*
- *Guide de déclinaison des mesures de sécurisation périmétrique et bâtimentaire ;*
- *Guide de prévention des atteintes aux personnes et aux biens en milieu de santé DGOS/ONVS ;*
- *Points clefs d'une politique de sécurité (document DGOS/FHF/MACSF) ;*
- *Politique de sécurité des systèmes d'information pour les ministères chargés des affaires sociales (PSSI MCAS)*[24] *;*
- *Politique générale de sécurité des systèmes d'information de santé (PGSSI-S)*[25] *:* ***référentiels et guides pratiques qui traitent de la sécurisation de données de santé ;***
- *Programme hôpital numérique ;*
- *Instruction n° SG/DSSIS/2016/309 du 14 octobre 2016relative à la mise en œuvre du plan d'action SSI.*

- **Ministère de l'intérieur**

- *Guide méthodologique de la vidéoprotection*[26] *(3 parties : démarche projet, étude de cas et fiches thématiques).*

- **Secrétariat général de la défense et de la sécurité nationale (SGDSN)**

- *Plan Vigipirate du 1*[er] *décembre 2016 « faire face ensemble »*[27]*.*

- **Normes**

- *ISO 31000 « Management du risque – Principes et lignes directrices » ;*
- *ISO 27001 « Management de la sécurité de l'information » ;*
- *ISO 28000 « Spécifications pour les systèmes de management de la sûreté pour la chaîne d'approvisionnement » ;*
- *ISO 27002 « Code de bonne pratique pour le management de la sécurité de l'information » ;*
- *Agence nationale de sécurité des systèmes d'information (ANSSI) : Guides des bonnes pratiques.*

- **Référentiels assurantiels du centre national de prévention et de protection**

- *Référentiel CNPP 1302 « Système de management de la sûreté - Lutte contre la malveillance et prévention des menaces » ;*
- *Référentiel APSAD R31 « Télésurveillance » ;*
- *Référentiel APSAD R81 « Détection d'intrusion » ;*
- *Référentiel APSAD R82 « Vidéosurveillance » ;*
- *Référentiel APSAD D83 « Contrôle d'accès » ;*
- *Référentiel CNPP 6011 « Analyse de vulnérabilité - Approche globale et méthode pour l'incendie ou la malveillance ».*

[24] Arrêté du 1er octobre 2015 portant approbation de la PSSI MCAS. NOR : AFSZ1523362A : https://www.legifrance.gouv.fr/eli/arrete/2015/10/1/AFSZ1523362A/jo/texte

[25] http://esante.gouvfr/

[26] http://www.interieur.gouv.fr/Videoprotection/Le-guide-methodologique/Les-3-parties-du-guide-methodologique

[27] http://www.sgdsn.gouv.fr/IMG/pdf/BROCHURE_VIGIPIRATE_GP-BD.pdf

6. Glossaire

ANSSI :	Agence nationale de la sécurité des systèmes d'information
ARS :	Agence régionale de santé
CHSCT :	Comité d'hygiène et de sécurité et des conditions de travail
CNAPS :	Conseil National des activités privées de sécurité
CRRA15 :	Centre de réception et de régulation des appels – Centre 15, voir SAMU
DGOS :	Direction générale de l'offre de soins
EEI :	Engin explosif improvisé
ERP :	Établissement recevant du public
ES :	Établissement de santé
ESPIC :	Établissement de santé privé d'intérêt collectif
FSI :	Forces de sécurité intérieure (police et gendarmerie nationales)
GAT :	Groupe d'appui technique sur la sécurité des établissements de santé (niveau ARS)
GN :	Gendarmerie nationale
HFDS :	Haut fonctionnaire de défense et de sécurité
IGH :	Immeuble de grande hauteur
NRBC-e :	Nucléaire, radiologique, bactériologique et chimique – explosif
OIV :	Opérateur d'importance vitale
ONVS :	Observatoire national des violences en milieu de santé
PCA :	Plan de continuité des activités
PIV :	Point d'importance vitale
PN :	Police nationale
PPP :	Plan particulier de protection
PSE :	Plan de sécurisation d'établissement
PSSI MCAS :	Politique de sécurité des systèmes d'information pour les ministères chargés des affaires sociales
PTI :	Protection du travailleur isolé
RAMSES :	Réception des alarmes et des messages des sites et établissements sensibles
RSSI :	Responsable de la sécurité des systèmes d'information
SAU :	Service d'accueil des urgences
SAMU :	Service d'aide médicale urgente
SGDSN :	Secrétariat général de la défense et de la sécurité nationale
SHFDS :	Service spécialisé du haut fonctionnaire de défense et de sécurité
SIC :	Systèmes d'information et de communication
SMUR :	Service mobile d'urgence et de réanimation
SSE :	Situation sanitaire exceptionnelle

7. Définitions

Accès	Voie de pénétration ou de passage dans une pièce ou un bâtiment via une issue ou un ouvrant. Un accès est dit facilement accessible lorsqu'il peut être atteint sans effort ou matériel particulier, par exemple à partir du sol, d'une terrasse, d'une toiture, d'une partie commune, d'un arbre, d'une construction contiguë quelconque, etc. Un accès est dit difficilement accessible, dans tous les autres cas.
Agression	Une agression est une attaque qui peut être physique ou verbale, active ou passive, directe ou indirecte.
Agent de sécurité	Employé formé et habilité à protéger/veiller (sur) les personnes et les biens contre la malveillance.
Alarme	Émission d'un signal sonore et/ou visuel pour prévenir les occupants d'un établissement d'un danger (d'origine malveillante ou accidentelle). Elle peut aussi ordonner l'évacuation en cas d'incendie. Elle peut donner lieu à une alerte.
Alerte	Action de demander l'intervention des services de sûreté (alerte interne) ou des services extérieurs : services de secours ou FSI (alerte externe).
Consigne	Attitude ou comportement attendu en réponse à un événement prédéterminé. La consigne répond à la question : quoi faire ?
Contrôle d'accès	Ensemble de moyens manuels ou automatiques permettant de s'assurer que l'accès à des espaces physiques ou des systèmes d'information est réservé à des personnes autorisées et ne pouvant, a priori, constituer une menace pour l'établissement.
Détection	La détection est périphérique lorsqu'elle consiste à surveiller l'approche extérieure d'une zone considérée. Elle concerne les clôtures matérielles ou immatérielles (barrières hyperfréquences, colonnes infrarouges, etc.) qui délimitent un espace. La détection périmétrique d'une installation est destinée à déceler, avant la pénétration à l'intérieur d'un bâtiment, la tentative d'ouverture ou de détérioration des issues, des ouvrants, des parois ainsi que des parties de parois de faible résistance mécanique du bâtiment. La détection intérieure permet de déceler une intrusion interne dans une pièce, un local, une partie ou la totalité d'un établissement. Elle peut être de quatre types : volumétrique, surfacique, linéaire ou ponctuelle.
Gestion des accès	Ensemble des techniques, moyens et procédures qui permettent de hiérarchiser les droits d'accès et éventuellement, d'assurer la traçabilité des accès à un site ou à des zones sensibles définies de ce site, allant du refus d'accès à la libre circulation complète. La gestion des accès peut être mécanique, humaine, électronique ou une combinaison de ces systèmes.
Intrusion	L'intrusion est le fait pour une personne de parvenir à accéder à une zone à laquelle elle n'a normalement pas accès.
Malveillance	Risque d'origine humaine, relevant d'une action ou d'une inaction volontaire dans l'intention de nuire à une personne, à un organisme ou à un bien.
Menace	En matière de malveillance, la menace est la résultante de plusieurs facteurs concourant à la concrétisation d'un préjudice ou d'un dommage, au détriment d'une personne, d'un organisme ou d'un bien. Les facteurs retenus sont généralement l'existence : - d'un objectif (aussi appelé cible) ; - d'un (ou plusieurs) auteur(s), qualifié(s) d'agresseur(s), de délinquant(s), de criminel(s) ; - d'un mode opératoire, fondé sur des méthodes et des moyens d'action.

Périmétrie	Ensemble des ouvertures d'un bâtiment par lesquelles un intrus est susceptible de pénétrer.
Poste central de sécurité ou de sûreté	Local disposant d'un personnel permanent, recevant et traitant à distance des messages d'alarme ayant pour origine des systèmes de détection d'intrusion, d'incendie, ou d'alarmes techniques du bâtiment. Il est également appelé poste de gardiennage, poste de sécurité ou poste de surveillance. Des normes spécifiques sont attachées à la conception et aux personnels de ce type de locaux.
Prévention	Prendre des mesures pour diminuer le nombre de faits.
Procédures	Ensemble d'actions et de manœuvres à exécuter, notamment par le recours à des moyens techniques, permettant l'application précise et correcte de la consigne. La procédure répond à la question : comment faire ?
Protection	Ensemble d'obstacles rendant ou empêchant la pénétration dans un site. Le principe repose sur une succession d'obstacles dressés devant l'attaquant visant à le dissuader, l'empêcher, le retarder et le retenir.
Résilience	« *Volonté et capacité d'un pays, de la société ou des pouvoirs publics à résister aux conséquences d'une agression ou d'une catastrophe majeures, puis à rétablir rapidement leur capacité de fonctionner normalement, ou à tout le moins dans un mode socialement acceptable* » (SGDSN).
Risque	Un risque se caractérise selon deux composantes : la probabilité d'occurrence d'un événement donné ; et la gravité des effets ou conséquences de l'événement pouvant se produire. Le risque résulte donc de la combinaison d'une menace, difficilement modifiable, et de l'exposition à cette menace qui, elle, peut-être maîtrisable.
Sécurité	La sécurité désigne l'ensemble des moyens humains, organisationnels et techniques réunis pour faire face aux risques techniques, physiques, chimiques et environnementaux pouvant nuire aux personnes et aux biens sans avoir un but de profit.
Sûreté	Ensemble des moyens techniques, humains et organisationnels visant à prévenir, empêcher et réduire la concrétisation d'un acte de malveillance. D'autres acceptations de ce terme sont à distinguer, notamment la notion de « sûreté de fonctionnement », mais également la notion de sûreté au sens juridique.
Surveillance	Action de contrôler et de vérifier de manière suivie des actions malveillantes visant des personnes ou des biens.
Système de vidéosurveillance	Un système de vidéosurveillance comprend nécessairement trois fonctions : la prise de vue (réalisée par le biais de caméras), la transmission (effectuée par un réseau), la restitution (visualisation sur moniteur). D'autres fonctions peuvent compléter un système : l'alarme (vidéo-détection), la conservation (enregistrement), etc.
Vidéoprotection	Terme d'usage utilisé par l'administration pour désigner les systèmes de vidéosurveillance répondant aux caractéristiques fixés par la réglementation en vigueur.
Vulnérabilité	En matière de malveillance, résultat de l'évaluation, pour un organisme, des possibilités d'atteinte d'une cible par une personne malintentionnée. L'évaluation des vulnérabilités de l'organisme correspond au processus d'évaluation des risques. La démarche d'évaluation des vulnérabilités s'appuie généralement sur une évaluation de la fréquence (probabilité) de concrétisation des menaces et de la gravité des conséquences en cas d'atteinte de la cible.

Contacts

Ministère des affaires sociales et de la santé

HFDS – Service spécialisé du haut fonctionnaire de défense et de sécurité
hfds@sg.social.gouv.fr

DGOS – Délégué pour la sécurité générale
sante.securite@sante.gouv.fr

14, avenue Duquesne – 75350 PARIS 07 SP