Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PRÉFET DE LA
HAUTE-GARONNE

- SIRACEDPC -

SÉCURISER UN SITE

FICHE A DESTINATION DES MAIRES ET DES RESPONSABLES DE SITES

Octobre 2018

FICHE VIGIPIRATE

1. LA DÉMARCHE GÉNÉRALE

Les sites à sécuriser sont ceux qui, en raison de leurs caractéristiques, sont **susceptibles d'être attractifs pour une action terroriste** :

- concentration ou flux importants de personnes (ex : établissements recevant du public, infrastructures de transport),
- concentration de personnes vulnérables (ex : établissements scolaires),
- valeur symbolique (ex : bâtiments officiels, lieux de culte),
- importance des installations qu'ils abritent (ex : sites Seveso, infrastructures de transport d'énergie).

Les principaux sites à sécuriser (liste non exhaustive) :

- Établissements recevant du public (ERP), notamment : établissements scolaires et d'enseignement, établissements de santé, sociaux et médico-sociaux, crèches et accueils de mineurs, centres commerciaux et grands magasins, salles de spectacle, cinémas, musées, stades...
- Sites liés aux culte : lieux de culte, établissements d'enseignement confessionnel, lieux communautaires...
- Sites institutionnels : administrations diverses, mairies, commissariats, gendarmeries, casernes, tribunaux, consulats...
- Sites touristiques
- Infrastructures de transport : aéroports-aérodromes, gares ferroviaires et routières, métro, tramway...
- Infrastructures de captage, transport et distribution d'énergie et d'eau, notamment : usines de production d'eau potable, sites de production d'électricité...
- Sites industriels, notamment Seveso
- Établissements de production ou de vente d'armes et munitions, dépôts d'explosifs
- Organes de presse et maisons d'édition

Outre les réglementations spécifiques s'appliquant à certains sites (établissements recevant du public, installations classées pour la protection de l'environnement...), **les mesures Vigipirate de vigilance,** prévention et protection face à la menace terroriste concernent l'ensemble des sites listés ci-dessus.

La démarche générale à mettre en œuvre dans ce cadre est la suivante :

- recenser les sites à sécuriser (mairies) ;
- constituer un annuaire permettant d'en contacter les responsables, y compris en cas d'urgence, afin de leur adresser des instructions dans le cadre du dispositif Vigipirate (mairies) ;
- sécuriser les sites au niveau adapté (mairies et responsables de site) ;
- développer des relations avec la mairie, les forces de l'ordre, le Service départemental d'incendie et de secours (SDIS) (responsables de site).

Il est utile, à l'échelle de la commune :

- d'identifier un référent chargé de veiller à la mise en œuvre du plan Vigipirate ;
- de faire réaliser des audits de sûreté sur les principaux sites municipaux.

Il est utile, à l'échelle du site :

- d'identifier un référent chargé de veiller à la mise en œuvre du plan Vigipirate ;
- de faire réaliser un audit de sûreté.

2. LES PRINCIPAUX RISQUES A PRENDRE EN COMPTE

- **attaque par arme(s) à feu, arme(s) blanche(s) ;**
- **véhicule bélier ;**
- **colis, véhicule ou personne piégé(e) ;**
- **cyberattaque**

Les risques spécifiques liés aux caractéristiques du site (ex : produits dangereux...) doivent également être pris en compte.

3. LES MESURES A METTRE EN ŒUVRE

Elles sont à adapter **en fonction des caractéristiques du site**.

Sur la base des principaux risques à prendre en compte, il s'agit d'**identifier les accès et moyens d'action possibles pour les terroristes**, et en déduire les mesures de prévention et de protection à mettre en oeuvre, selon une logique consistant à:

DÉTECTER – PROTÉGER – ALERTER - RETARDER.

La **prise en compte constante** des exigences de sécurisation dans l'organisation du site permet d'en limiter le coût.

3.1. Les restrictions de circulation et de stationnement

Elles ont pour objet de **prévenir les risques liés à un véhicule bélier ou véhicule piégé**. Elles facilitent l'ensemble des mesures à mettre en œuvre pour sécuriser le site et ses abords (contrôle d'accès, surveillance interne et externe, protections passives).

Mesures :

- restriction de circulation et de stationnement des véhicules dans le site ;
- restriction de circulation (notamment poids-lourds) et stationnement des véhicules aux abords du site par arrêté municipal.

Le périmètre de sécurité à mettre en place en cas de véhicule suspect est de **200m** (effets amplifiés sous un pont ou dans un espace cerné de murs ou de bâtiments). Cet ordre de grandeur doit être considéré pour dimensionner les restrictions.

Préconisations sur la mise en œuvre des mesures :

- éloigner la circulation et le stationnement non contrôlés du site ;
- contrôler les véhicules devant accéder au site ou ses abords (badges, macarons, procédure d'accès pour les visiteurs, livraisons, intervenants extérieurs...) ;
- faire respecter les restrictions de circulation et de stationnement (obstacles physiques, signalement et enlèvement des véhicules contrevenants...) ;
- distinguer, dans la mesure du possible, les accès piétons des accès véhicules.

3.2. Le contrôle d'accès

Il a pour objet d'éviter l'introduction dans le site d'objets ou véhicules dangereux.

Mesures :

- filtrage des personnes et véhicules (ouverture commandée, badges, procédure d'accès pour les visiteurs, livraisons, intervenants extérieurs...) ;
- inspection visuelle voire fouille des sacs et bagages ;
- demande d'ouverture des manteaux et vestes ;
- inspection visuelle des véhicules ;
- utilisation de magnétomètres, portiques ;
- palpations de sécurité ;
- filtrage du courrier entrant (notamment colis).

Préconisations sur la mise en œuvre des mesures :

- veiller à l'efficacité et l'intégrité des clôtures, portes et portails ;
- limiter, dans la mesure du possible, le nombre des accès au site, en préservant la possibilité d'évacuer ;
- veiller à la fluidité des accès, afin d'éviter des engorgements qui constitueraient des vulnérabilités en périphérie du site (par le dimensionnement correct des moyens de contrôle d'accès, l'assouplissement des horaires...) ;
- séparer les flux entrant et sortant, les piétons et les véhicules ;
- définir une procédure d'accès pour les visiteurs, les livraisons, les intervenants extérieurs (enregistrement, demande de pièce d'identité ou justificatif, badge, accompagnement...) ;
- prévoir un système de consigne pour les objets interdits sur le site ;
- interdire les "détournements d'usage" des accès (accès déverrouillés pour servir de raccourci, d'accès aux espaces extérieurs pour les fumeurs...) ;
- veiller au maintien de la qualité des contrôles (notamment : supervision et relèves pour les agents de sécurité) ;
- veiller à disposer d'agents de sécurité femmes pour la réalisation des palpations de sécurité sur les femmes ;
- veiller à l'application des mesures aux enfants (le contrôle peut leur être expliqué et avoir une dimension pédagogique) ;
- veiller à l'identification des agents de sécurité : liste, tenue spécifique ;
- définir une procédure de traitement du courrier entrant, notamment des colis (enregistrement des dépôts par coursier, vérification auprès des destinataires qu'un colis est attendu, ouverture dans des locaux non ventilés...).

Le délai de réalisation du contrôle d'accès est estimé à **45 secondes** en moyenne par personne (accueil, palpations de sécurité, inspection visuelle du sac, transition d'une personne à une autre), soit 40 personnes par agent de sécurité par demi-heure. Le dispositif doit être dimensionné en fonction des caractéristiques du site (afflux massif à des horaires donnés).

Les outils suivants facilitent le contrôle d'accès et peuvent utilement être développés : commande d'ouverture des principaux accès, interphone, visiophone…

Documents utiles : affiches et logos Vigipirate
www.haute-garonne.gouv.fr/risqueterroriste

RAPPELS RÉGLEMENTAIRES SUR LE CONTRÔLE D'ACCÈS

Les mesures de contrôle d'accès, et le cadre dans lequel elles s'inscrivent (Vigipirate), doivent être signalés aux personnes accédant au site (affiches, règlement intérieur...).

Les mesures d'inspection visuelle des sacs et bagages, des personnes (demande d'ouverture des vestes et manteaux), des véhicules (ouverture des portières, du coffre, utilisation d'un miroir d'inspection) sont réalisées avec le consentement des intéressés, sans contact entre la personne réalisant l'inspection et les sacs, bagages, personnes ou véhicules concernés. L'accès doit être refusé aux personnes qui refusent de s'y soumettre.

Les mesures de fouille ou palpations des sacs, bagages et personnes sont réalisées par des agents de sécurité disposant d'un agrément spécifique délivré par le Conseil national des activités privées de sécurité (CNAPS), avec le consentement des intéressés. Les palpations de sécurité sur les personnes sont réalisées par un agent de sécurité du même sexe que l'intéressé. L'accès doit être refusé aux personnes qui refusent de s'y soumettre.

La réglementation prévoit la possibilité de soumettre l'accès aux enceintes dans lesquelles sont organisées des manifestations sportives, récréatives ou culturelles rassemblant plus de 300 spectateurs à des mesures de fouille et palpations des sacs, bagages et personnes, sous le contrôle d'un Officier de police judiciaire (OPJ). La présence de cet OPJ n'est pas nécessaire durant la mise en œuvre des mesures. L'exigence de contrôle d'un OPJ est remplie dès lors que le rassemblement et le dispositif sont signalés à la police ou la gendarmerie.

Les contrôles d'identité relèvent des forces de l'ordre, ainsi que la fouille des véhicules, sur réquisition du Procureur de la République.

Informations utiles sur les activités privées de sécurité : http://www.cnaps-securite.fr/ 01.48.22.20.40

3.3. La surveillance interne et externe

Elle a pour objet de détecter et signaler les comportements et objets/colis suspects dans le site et aux abords.

Mesures :

- organisation de rondes de surveillance d'agents de sécurité et autres personnels ;
- organisation de patrouilles de police municipale lorsqu'elle existe.

Préconisations sur la mise en œuvre des mesures :

- privilégier les rondes et patrouilles dynamiques et aléatoires ;
- identifier et sécuriser les points hauts (ex : immeuble surplombant…) ;
- restreindre l'accès aux locaux (techniques, de stockage...), avec une attention particulière sur la gestion des clés, badges, codes d'accès, plans des locaux ;
- limiter les points possibles de dépose d'un colis piégé (par exemple : conteneurs verre, conteneurs poubelle, accumulations d'objets...).

Le périmètre à mettre en place autour d'un colis suspect est de **100m** (effets amplifiés sous un pont ou dans un espace cerné de murs ou de bâtiments). Cet ordre de grandeur doit être considéré pour dimensionner les mesures de surveillance aux abords du site.

Les outils suivants facilitent la surveillance et peuvent utilement être développés : éclairage, vidéoprotection, alarmes liées à des détecteurs de présence et d'intrusion, barreaux sur fenêtres en rez-de-chaussée, miroirs d'angle, supports de sacs poubelle transparents...

NB :

- La possibilité pour des communes de mettre en commun des agents de police municipale existe et peut être étudiée (cf. VII - Références réglementaires) ;
- L'autorisation pour des agents de sécurité de réaliser des rondes sur le domaine public existe et peut être demandée au Préfet.

Ces mesures peuvent être complétées :

- des patrouilles dynamiques de police ou de gendarmerie ;
- dans le cas de sites identifiés comme prioritaires, des patrouilles de militaires dans le cadre du dispositif "Sentinelle" sur décision de la préfecture.

Informations sur la vidéoprotection :
http://www.interieur.gouv.fr/Videoprotection
http://www.haute-garonne.gouv.fr/Politiques-publiques/Securite-et-protection-des-personnes-et-des-biens/Securite-interieure/Video-protection

3.4. Les protections passives

Elles protègent le site en ralentissant ou faisant obstacle à un véhicule bélier.

Mesures :

- pose d'obstacles en point d'arrêt ou en chicane sur les voies de circulation ;
- pose d'obstacles protégeant des couloirs ou zones réservés aux piétons ;
- pose d'obstacles protégeant des produits dangereux (stockage de bouteilles de gaz...).

Préconisations sur la mise en œuvre des mesures :

- identifier et protéger les vulnérabilités du site : file d'attente extérieure, espace vitré proche d'une voie de circulation... ;
- utiliser des obstacles suffisamment résistants pour garantir l'effectivité de la protection contre un véhicule bélier (y compris un poids-lourd) : murs béton, plots béton, sacs de sable type "big bag", bastion walls, mais également fossés, tranchées ;
- traiter les deux sens de circulation (véhicule bélier susceptible d'emprunter un sens interdit) ;
- positionner les obstacles de manière à arrêter ou ralentir un véhicule, y compris un deux-roues, tout en préservant la possibilité pour les piétons de circuler, notamment en cas d'évacuation.

Document utile : schéma indicatif d'implantation de murs béton (en annexe)

3.5. Les procédures d'alerte et de réaction en cas d'attaque terroriste

Ces procédures doivent être définies. Elles peuvent s'appuyer sur les préconisations nationales en matière de conduite à tenir en cas d'attaque.

Mesures :

- définition d'une procédure d'alerte en cas d'attaque terroriste ;
- définition d'une procédure de réaction en cas d'attaque terroriste.

Préconisations sur la mise en œuvre des mesures :

- définir une procédure d'alerte par le personnel du site (alerte montante) ainsi qu'une procédure permettant l'alerte du personnel et des visiteurs du site (alerte descendante) ;
- distinguer le système d'alerte "attaque terroriste" du système d'alerte en cas d'évacuation incendie : utilisation d'une sonnerie différente (codée, modifiée...), sonorisation ;
- définir une procédure de réaction : itinéraires d'évacuation, lieux de mise en sûreté (réserves, toilettes, toits...) ;
- vérifier régulièrement la disponibilité des itinéraires d'évacuation ;
- protéger et équiper les lieux de mise en sûreté ;
- protéger et équiper le Poste de commandement (PC) sécurité lorsqu'il existe ;
- formaliser les procédures d'alerte et de réaction dans un plan (ex : Plan particulier de mise en sûreté pour les établissements scolaires...) ;
- constituer un annuaire de crise ;
- s'assurer de la disponibilité de plans des locaux à fournir aux services intervenants en cas d'attaque terroriste ;
- s'assurer de la continuité des transmissions, notamment en cas d'interruption du réseau de téléphonie mobile (utilisation de matériel radio, téléphonie fixe...) ;
- tester le dispositif (alerte, réaction) à l'occasion d'exercices réguliers et progressifs (ex : pour les établissements scolaires, 3 exercices destinés à tester le PPMS par an dont 1 exercice "attentat intrusion") ;
- réaliser un retour d'expérience après chaque exercice ou alerte afin d'améliorer les procédures.

Les outils suivants facilitent l'alerte et la réaction et peuvent utilement être développés : sonnerie d'alerte distincte de la sonnerie incendie, sonorisation, écrans de projection, boutons poussoirs d'alerte, commande de fermeture des principaux accès, portes blindées, dispositifs de blocage de porte, protections balistiques des lieux de mise en sûreté, film anti déflagrant pour vitres, matériel de transmission radio…

En complément, il est recommandé aux utilisateurs de Twitter de s'abonner au nouveau compte @Beauvau_alerte et d'en activer les notifications afin d'être informé en cas d'événement majeur de sécurité publique ou civile et de recevoir des consignes comportementales adaptées.

Informations utiles sur la conduite à tenir en cas d'attaque terroriste :
http://www.gouvernement.fr/reagir-attaque-terroriste

Informations utiles sur le dispositif d'alerte du Gouvernement :
https://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Alerte-et-informations-a-la-population

Documents utiles : guides, affiches et logos Vigipirate
www.haute-garonne.gouv.fr/risqueterroriste

RAPPELS SUR LES RÉACTIONS A ADOPTER EN CAS D'ATTAQUE TERRORISTE

Dans tous les cas :

- caractériser la situation (où ? quoi ? qui ?) ;
- déterminer la réaction appropriée ;
- alerter le personnel et les visiteurs du site ;
- alerter les forces de l'ordre (17, 112 ou 114 pour les personnes ayant des difficultés à entendre et à parler) ;
- alerter les sites voisins ;
- stopper les flux entrants et dissuader les personnes de se diriger vers la zone de danger ;
- obéir aux forces de l'ordre, sans diffuser d'informations sur leurs modalités d'intervention ;
- faciliter l'action des secours (signaler les blessés) ;
- être attentifs aux personnes stressées, vulnérables ;
- ne pas diffuser de rumeurs.

Si l'attaque est extérieure au site : il est préférable de confiner le personnel et les visiteurs au sein des locaux, en diffusant un message d'information pour éviter un mouvement de panique.
Si l'attaque a lieu à l'intérieur du site : les mesures d'évacuation ou de confinement doivent être envisagées en fonction des sites et des circonstances.

La situation n'est pas figée, elle évolue. Les procédures de réaction doivent s'adapter aux circonstances.

Consignes d'évacuation ("S'échapper") :

- localiser le danger pour s'en éloigner par le plus court chemin ;
- si possible, aider les autres personnes à s'échapper ;
- ne pas s'exposer ;
- dissuader les personnes de pénétrer dans la zone de danger ;
- évacuer calmement, mains levées apparentes.

Consignes de confinement/mise en sûreté ("Se cacher") :

- s'enfermer et se barricader à l'aide des objets disponibles ;
- éteindre la lumière et couper le son des appareils ;
- s'éloigner des ouvertures et s'allonger au sol ;
- faute de lieu de mise en sûreté, s'abriter derrière un obstacle (mur, pilier...) ;
- couper la sonnerie et le vibreur des téléphones.

3.6. Les premiers secours

La formation du personnel aux premiers secours est à favoriser.

Informations utiles :
www.haute-garonne.gouv.fr/secourisme

3.7. La sensibilisation du public et du personnel

Elle vise à expliquer les mesures, faciliter leur mise en œuvre, favoriser le signalement des comportements et objets/colis suspects et la connaissance des procédures d'alerte et de réaction en cas d'attaque terroriste.

Mesures :

- sensibilisation du personnel ;
- sensibilisation des visiteurs.

Préconisations sur la mise en œuvre des mesures :

- moyens de sensibilisation du personnel : affiches, règlement intérieur, consignes écrites, guides, réunions...
- thèmes de sensibilisation du personnel :
  - vigilance vis-à-vis des comportements, objets/colis suspects (prévoir une procédure de signalement) ;
  - procédures d'alerte et de réaction ;
  - n° d'urgence ;
- favoriser la connaissance du site en organisant des reconnaissances exploratoires (itinéraires d'évacuation, lieux de mise en sûreté) et des exercices ;
- informer les représentants du personnel, le Comité d'hygiène et de sécurité des conditions de travail (CHSCT) ;

- moyens de sensibilisation des visiteurs : affiches, sonorisation, tickets, réunions (ex : parents d'élèves avant la rentrée)...
- thèmes de sensibilisation des visiteurs :
  - nécessité de se soumettre aux contrôles et les faciliter, notamment en évitant sacs et bagages, objets interdits (bouteilles, objets tranchants, casques...) ou encore en anticipant l'arrivée sur site (cas des salles de spectacle, des stades...) ;
  - nécessité d'éviter les attroupements devant les accès au site (cas des établissements scolaires au moment de la dépose ou la récupération des enfants...) ;
  - ne pas laisser ses effets personnels sans surveillance, car ils pourraient être considérés comme suspects ;
  - vigilance vis-à-vis des comportements, objets/colis suspects (prévoir une procédure de signalement) ;
  - procédures d'alerte et de réaction ;
  - n° d'urgence.

Documents utiles :
guides, affiches et logos Vigipirate (www.haute-garonne.gouv.fr/risqueterroriste)

RAPPELS SUR LES COMPORTEMENTS / ÉLÉMENTS SUSPECTS

Ces comportements/éléments doivent alerter et sont à signaler aux forces de l'ordre :

- attitudes laissant supposer un repérage (curiosité inhabituelle relative aux mesures de sécurité, à l'organisation, allées et venues, observation prolongée, prise de photos ou vidéo, personne ou véhicule stationnant de manière prolongée au même endroit, avec ou sans occupant...) ;
- menaces verbales, tags menaçants, appels téléphoniques malveillants ;
- véhicule stationné à proximité du rassemblement sur un emplacement inapproprié ;
- sous-traitants, livreurs intervenant en dehors des lieux et horaires habituels ;
- sac abandonné, objet/colis suspect ;
- tenue vestimentaire inhabituelle pour la saison (ex : manteau en été).

En cas de découverte d'un objet/colis suspect :

- alerter les forces de l'ordre (en composant le 17) ;
- éloigner les personnes de l'objet/colis ;
- ne pas manipuler, ni déplacer l'objet/colis suspect.

3.8. La cybersécurité

Une attention particulière doit être portée à la sécurité des systèmes d'information et de communication, ou cybersécurité.

Liens utiles :
Conseils aux usagers en matière de cybersécurité :
http://www.gouvernement.fr/risques/conseils-aux-usagers
Objectifs de cybersécurité du plan Vigipirate sur le site de l'Autorité nationale de sécurité des systèmes d'information (ANSSI) :
http://www.ssi.gouv.fr/agence/cybersecurite/plans-gouvernementaux/

4. L'EXIGENCE DE DISCRÉTION

Il est essentiel d'observer la grande discrétion sur les dispositifs de sécurisation mis en place afin de **ne pas divulguer d'éléments utiles à la réalisation d'une action malveillante**.

NB : Le floutage d'un site peut être demandé par son responsable aux gestionnaires d'applications géographiques telles google earth, maps, street view...

5. LES INTERLOCUTEURS A IDENTIFIER

Les **relations et partenariats** suivants sont à développer par les responsables de sites :

- Mairies (notamment référent Vigipirate, police municipale) ;
- Forces de l'ordre : commissariat de quartier ou brigade de gendarmerie compétente, ou référents désignés (ex : référents écoles de la police et la gendarmerie) ; attention, en cas d'urgence, composer le 17 ;
- SDIS : Centre d'incendie et de secours (CIS) compétent ; attention, en cas d'urgence, composer le 18 ;
- Interlocuteurs ministériels de niveau départemental, zonal, national :
  - correspondants Vigipirate dans les services "référents" désignés par le Préfet au niveau départemental : Agence régionale de santé (ARS), Direction départementale de la cohésion sociale (DDCS), Direction départementale de la protection des populations (DDPP), Direction départementale des territoires (DDT), Direction régionale de l'agriculture, de l'alimentation et de la forêt (DRAAF), Direction régionale des affaires culturelles (DRAC), Direction régionale de l'environnement, de l'aménagement et du logement (DREAL), Direction régionale des finances publiques (DRFIP), Direction régionale de la jeunesse, des sports et de la vie associative (DRJSCS), Direction de la sécurité de l'aviation civile Sud (DSAC Sud), Rectorat/Direction académique des services de l'éducation nationale (DASEN), services locaux du ministère de la justice ;
  - interlocuteurs locaux spécifiques (ex : équipe mobile de sécurité Rectorat/DASEN) ;
- Référents sécurité désignés par les autorités cultuelles ;
- Préfecture :
  - Cabinet - Service interministériel régional des affaires civiles et économiques de défense et de protection civile (SIRACEDPC) : mise en œuvre de Vigipirate ;
  - Cabinet - Service des politiques de prévention et de sécurité (SP2) : vidéoprotection, Fonds interministériel de prévention de la délinquance (FIPD).

DOCUMENTS ET LIENS UTILES

L'ensemble des documents, informations et liens utiles figure sur la page "Vigipirate" de l'Internet de l'État en Haute-Garonne (www.haute-garonne.gouv.fr/risqueterroriste) :

- lien vers le plan gouvernemental Vigipirate ;
- lien vers le Dossier départemental des risques majeurs (DDRM) et le modèle de Document d'information communal sur les risques majeurs (DICRIM) ;
- fiches mesures Vigipirate ;
- affiches ;
- logos et instructions d'utilisation ;
- guides ;
- liens utiles.

RÉFÉRENCES RÉGLEMENTAIRES

- Code général des collectivités territoriales (pouvoir de police du maire) : articles L2212-1 et 2 ;
- Code général des collectivités territoriales (pouvoir de police du Préfet) : articles L2214-4, L2215-1 ;
- Code de la sécurité intérieure (activités de surveillance et de gardiennage) : articles L613-1 et suivants ;
- Code pénal : article 223-1 (exposition d'autrui à un risque par violation manifestement délibérée d'une obligation particulière de sécurité ou de prudence) ;
- Code de la sécurité intérieure (mutualisation des agents de police municipale) : articles L512-1, L511-4 et suivants, R2212-11 à R2212-14 ;
- Plan gouvernemental Vigipirate (partie publique) : https://www.gouvernement.fr/risques/menace-terroriste;
- Réglementation applicable aux ERP ;
- Code de l'éducation (pouvoir du chef d'établissement) : articles R421-10 et R421-12 ;
- Textes du ministère de l'éducation nationale, de l'enseignement supérieur et de la recherche : http://www.education.gouv.fr/cid85267/consignes-de-securite-applicables-dans-les-etablissements-relevant-du-ministere.html

Annexe 1

Grille de vérification de la sécurisation d'un site	Oui/Non
1)Le site est-il connu de la mairie ? De la police ou la gendarmerie ? Du SDIS ?	
2) Des partenariats sont-ils developpés avec ces interlocuteurs ?	
3) Les principaux risques sont-ils pris en compte (attaque par arme(s) balistique(s) ou arme(s) blanche(s) ; véhicule bélier ; colis, véhicule ou personne piégé(e) ; cyber-attaque) ?	
4) Des restrictions de circulation et de stationnement sont-elles prises ?	
5) Un dispositif de contrôle d'accès (filtrage, inspection visuelle des sacs, palpations...) est-il en place ?	
6) Un dispositif de surveillance interne et externe (vidéoprotection, rondes d'agents de sécurité, patrouilles de police municipale...) est-il en place ?	
7) Des protections passives (murs béton, fossés...) sont-elles en place ?	
8) Le personnel est-il formé aux premiers secours ?	
9) Des procédures d'alerte et de réaction en cas d'attaque terroriste sont-elles déterminées ?	
10) Les plans du site sont-ils disponibles en cas d'intervention ?	
11) L'annuaire de crise est-il élaboré ?	
12) Le personnel et les visiteurs du site sont-ils sensibilisés ?	
13) Des reconnaissances exploratoires du site, des exercices sont-ils réalisés ?	
14) Les comportements et éléments suspects à signaler aux forces de l'ordre sont-ils connus ?	
15) Une attention particulière est-elle portée à la cybersécurité ?	
16) L'exigence de discrétion sur le dispositif de sécurisation du site est-elle respectée ?	
17) Un retour d'expérience est-il réalisé après chaque exercice ou incident ?	

Annexe 2 : Préconisations opérationnelles sur les protections passives

Le dispositif doit s'adapter au terrain.

Différentes possibilités de positionnement des murs béton (en « couloirs », en quinconce).

Veiller à ce que le dispositif empêche l'intrusion d'un véhicule bélier y compris par les trottoirs ou tout autre espace laissé libre en dehors de la voie proprement dite.

Positionner, dans la mesure du possible, les murs béton par 2, liés entre eux (un mur béton isolé peut pivoter sous le choc d'un véhicule bélier).

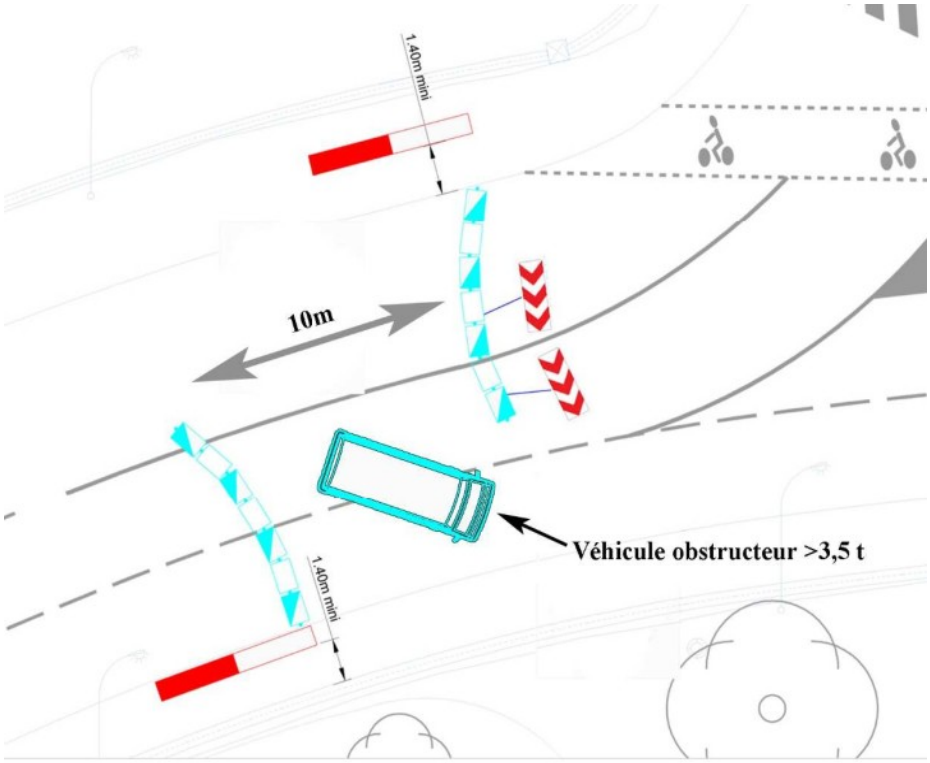

Schéma indicatif de chicane fermée (protection passive contre le risque de véhicule bélier avec possibilité d'accès pour des véhicules autorisés, notamment ceux des services d'intervention et de secours) :
- prévoir un espacement de 10m entre les protections passives constituant la chicane
- prévoir un véhicule obstructeur pour la fermeture de la chicane (amovible : conducteur et clés à proximité), dans la mesure du possible, de plus de 3,5 tonnes.