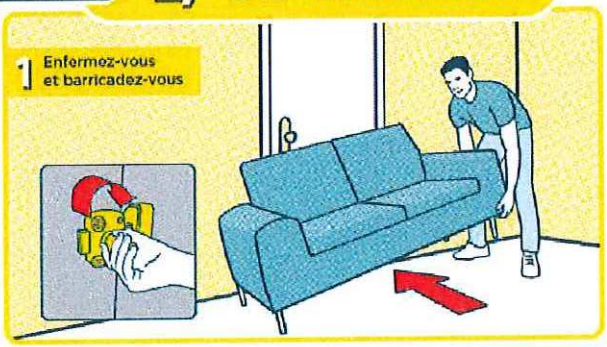
Annexe 1 : **LOGO et affiche à apposer**

RÉAGIR EN CAS D'ATTAQUE TERRORISTE

AVANT L'ARRIVÉE DES FORCES DE L'ORDRE, CES COMPORTEMENTS PEUVENT VOUS SAUVER

1/ S'ÉCHAPPER *si c'est impossible* 2/ SE CACHER



3/ ALERTER
ET OBÉIR AUX FORCES DE L'ORDRE

Dès que vous êtes en sécurité, appelez le 17 ou le 112

Gardez les mains levées et ouvertes

VIGILANCE

- Témoin d'une situation ou d'un **comportement suspect**, vous devez contacter les forces de l'ordre **(17 ou 112)**
- Quand vous entrez dans un lieu, repérez les **sorties de secours**

- Ne diffusez aucune information sur l'intervention des forces de l'ordre
- Ne diffusez pas de rumeurs ou d'**informations non vérifiées** sur Internet et les réseaux sociaux
- Sur les réseaux sociaux, **suivez les comptes @Place_Beauvau et @gouvernementfr**

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Pour en savoir plus :
www.gouvernement.fr/reagir-attaque-terroriste

VIGIPIRATE

Annexe 2 : Extraits de la partie publique du plan

1.2. Directeurs et responsables de sites accueillant du public, comment vous préparer ?

Tout responsable d'établissement recevant du public est encouragé à décliner VIGIPIRATE dans son propre plan de sûreté d'entreprise. Ce plan prévoit les mesures à prendre en cas de menace ou d'attentat, ou simplement de risques tels que la découverte d'objets abandonnés.

Il fixe les dispositions spéciales à appliquer en matière de surveillance, d'organisation et de contrôle. Chaque agent de la société est informé de ce qu'il doit faire dans le cadre du plan d'entreprise.

L'Etat encourage particulièrement les établissements recevant du public à **établir des procédures de réaction en cas d'attaque terroriste et à sensibiliser leurs employés.**

A cette fin, les autorités ont préparé, en liaison avec les acteurs concernés, un ensemble de **guides de bonnes pratiques**[12] à destination des responsables d'établissements recevant du public, qui présentent les comportements individuels et collectifs à adopter pour se préparer à une attaque terroriste.

Une bonne organisation préalable de vos établissements ainsi qu'une réaction adaptée des personnels peuvent sauver des vies.

1.2.1. Préparer son organisation à un acte de malveillance ou de terrorisme

De nombreux conseils sont délivrés ci-dessous. Certains peuvent être difficilement applicables par l'ensemble des sites. Ils doivent donc être adaptés en fonction de la situation.

a) Développer les relations avec les partenaires extérieurs

Les différents partenaires extérieurs :

- **le préfet et les services préfectoraux.** Ils évaluent le niveau de la menace et établissent les mesures de vigilance et de protection à adopter dans le cadre de la mise en œuvre du plan VIGIPIRATE ;
- **le maire et les services municipaux.** Ils complètent l'action des forces de police et de gendarmerie. Ils procèdent aux aménagement de voie publique nécessaires à la protection des installations exposées ;
- **les forces de police et de gendarmerie.** Elles peuvent, en s'appuyant sur leurs référents sûreté, apporter des conseils de sécurité aux responsables de site sur le renforcement de leurs mesures de sécurité. Des rencontres régulières avec les forces de police et de gendarmerie participent de la connaissance mutuelle. Pour les sites représentant une sensibilité particulière, des plans des bâtiments peuvent être remis aux forces de sécurité afin de faciliter une intervention en cas d'attaque.

12- Voir les guides sectoriels de bonnes pratiques sur http://www.gouvernement.fr/reagir-attaque-terroriste

b) Analyser les vulnérabilités de son établissement

- identifiez en quoi votre établissement pourrait être une cible (lieu de grands rassemblements de personnes, site représentant les institutions du pays, site symbolique du mode de vie occidental ou des valeurs de la République française, lieu de culte, etc.) ;
- identifiez ce qui pourrait être ciblé dans votre établissement : personnels, infrastructures, informations, produits ou matériels spécifiques qui pourraient être volés en vue d'une action terroriste ;
- identifiez les vulnérabilités physiques de l'établissement (nombre d'accès, portes ne fermant pas à clef, accès livraison non surveillés, etc.) ;
- envisagez les moyens d'action possibles (arme blanche, arme automatique, voiture-bélier, colis ou véhicule piégé) ;
- prenez en compte la menace interne (radicalisation pouvant devenir violente par exemple).

c) S'organiser

Renforcer la protection du site :

- limitez le nombre d'accès pour une meilleure surveillance des flux sans réduire la capacité d'évacuation de vos employés et du public ;
- déployez un système de vidéo-protection ;
- mettez en place un système de badges d'accès ;
- installez un système d'interphone, si possible avec caméra ;
- faites en sorte que les portes d'accès au site soient éclairées ;
- changez régulièrement les codes des claviers alphanumériques de type Digicode ;
- mettez en place un système de filtrage et de fouille aux accès ;
- protégez l'accès extérieur du site de toute possibilité d'attaque d'un véhicule-bélier (mise en place de plots, bacs de fleurs, blocs de béton, herses mobiles, etc.) ;
- coordonnez-vous avec les établissements ou les entreprises limitrophes ;
- faites en sorte que les parties communes et les zones techniques du site soient maintenues propres et qu'on ne puisse pas y dissimuler de colis abandonnés ;
- vérifiez la disponibilité des issues de secours.

Mettre en place des moyens d'alerte spécifiques :

- *Alerter au sein de l'organisation.* **Il est essentiel que chaque organisation puisse donner l'alerte en cas d'attaque terroriste.** Le système d'alerte conditionne la réaction de l'ensemble des personnes occupant le site et doit être distinct de l'alarme incendie car la réaction attendue n'est pas la même. Un tel système ne s'improvise pas et il est recommandé de l'établir en concertation avec le personnel de l'établissement. Ces moyens d'alerte doivent être connus de tous et testés régulièrement à l'occasion de mises en situation et d'exercices.
- Pour que la procédure d'alerte soit complète, il faut mettre en place deux systèmes :
  - **un système d'alerte décentralisé** qui permette à chacun de donner l'alerte une fois l'acte de malveillance constaté (sifflet, téléphone fixe, SMS téléphonique, système de bipeur, radio, etc.) ;
  - **un système d'alerte centralisé** qui permette de prévenir l'ensemble du site (surtout s'il est étendu) : alarme sonore distincte de l'alarme incendie, message par haut-parleur, avertisseur lumineux, SMS téléphonique, corne de brume, etc.

- **L'alerte a pour vocation de prévenir d'une attaque.** Idéalement, deux types d'attaques doivent être distingués car ils n'appellent pas les mêmes réactions :
  - l'attaque extérieure au site et à proximité (confinement recommandé) ;
  - l'attaque dans le site (évacuation ou confinement en fonction de la localisation des personnes dans le bâtiment). **Il n'est pas recommandé d'imposer une réaction unique pour l'ensemble du site concerné, en cas d'attaque interne.** Certaines personnes peuvent facilement s'échapper du fait de la situation de leurs locaux, d'autres ne peuvent pas fuir facilement et doivent donc se confiner. Il est, par conséquent, préférable de laisser l'initiative aux personnes occupant le site.

Pour distinguer les deux types d'attaques (interne et externe), des codes sonores ou visuels différents peuvent être employés. Par exemple, une attaque extérieure pourra être signalée par 3 longues sonneries alors qu'une attaque sur le site pourra être signalée par 6 longues sonneries. De même, si l'alerte est donnée par SMS, le message doit préciser si l'attaque est interne ou externe au site.

- *Alerter hors de l'organisation :* forces de sécurité, établissements extérieurs sensibles (hôpitaux, écoles, etc.). **Plus vite l'alerte est donnée et plus vite les forces de sécurité intérieure peuvent intervenir.**
- Sensibilisez vos employés au fait que chacun doit se sentir responsable et doit prévenir en cas d'attaque. Le message à faire passer est le suivant : **« ne pensez pas que d'autres ont donné l'alerte, faites-le ».**

Préparer :

- une **mallette de crise** avec les numéros de téléphone des personnes à joindre et les plans du site qui pourraient être remis aux forces de sécurité en cas d'attaque ;
- des **procédures de réaction adaptées** aux différents actes de malveillance :
  - alerte à la bombe (privilégier la même réaction qu'une alerte incendie) ;
  - attaque à l'intérieur du site (évacuation ou confinement) ;
  - attaque à l'extérieur mais à proximité du site (confinement privilégié) ;
- des **itinéraires d'évacuation** (ce ne sont pas forcément les issues de secours, un toit peut faire office de protection par exemple) ;
- des **pièces de confinement** connues de tous. Les fermetures des portes peuvent être renforcées à moindre coût.

Sensibiliser le personnel :

Informer le personnel :

- informez les agents sur la menace et sur les différentes bonnes pratiques à avoir dans un contexte de menace terroriste ;
- **développez une stratégie de sensibilisation interne** en apposant l'affiche (*voir page 6*) et en diffusant la vidéo « Réagir en cas d'attaque terroriste »[13]. Les guides de bonnes pratiques propres à certains secteurs professionnels peuvent également être distribués ;
- sensibilisez le personnel au respect des mesures de sécurité et de vigilance ;
- **rappelez les procédures et le rôle de chacun ;**
  - informez les agents sur la procédure de signalement de comportements suspects (employé manifestant une pensée extrême, potentiellement violente) ;
  - encouragez la vigilance des employés afin de détecter et de signaler les comportements suspects.

13- Voir le site http://www.gouvernement.fr/reagir-attaque-terroriste

Former le personnel :

- encouragez la formation aux premiers secours ;
- assurez-vous de la connaissance et de la maîtrise par tous des moyens d'alerte ;
- favorisez la connaissance du site en organisant des « reconnaissances exploratoires » afin d'identifier les cheminements, les issues de secours, les obstacles éventuels, et tout ce qui peut offrir une protection ;
- organisez des mises en situation simples et des exercices collectifs, intégrant éventuellement les différents partenaires, et en exploitant systématiquement les retours d'expérience de ces exercices.

3. PROTÉGER LES INSTALLATIONS ET BÂTIMENTS

Description du domaine

Le domaine des installations et bâtiments concerne **l'ensemble des édifices qui peuvent constituer des cibles potentielles, soit en raison de leur valeur symbolique, économique, politique ou écologique, soit en raison du public qu'ils accueillent.** Certaines infrastructures propres à des secteurs d'activités précis font l'objet de protections spécifiques, décrites dans les chapitres du plan VIGIPIRATE classifié qui leur sont consacrés. C'est le cas pour les transports, les installations dangereuses, les réseaux, la chaîne alimentaire et la santé.

Les pouvoirs publics sont chargés de la protection externe, qu'ils assurent notamment par la surveillance de la voie publique et la régulation de la circulation et du stationnement. Le dispositif est adapté en fonction du type d'installation, de sa configuration et de l'évaluation de la menace. Il peut employer des forces de l'ordre de nature différente : les services locaux, les polices municipales, la police nationale, la gendarmerie nationale, voire les armées.

Les responsables d'installations et bâtiments sont chargés de la protection interne et des accès aux bâtiments.

Stratégie de sécurité

La stratégie vise à **adapter la sécurité externe, en agissant sur la surveillance et sur les conditions de stationnement et de circulation aux abords des installations, la sécurité des accès et la sécurité interne, en agissant sur la surveillance et le contrôle des flux.** Elle s'appuie sur les principes de défense en profondeur et de responsabilité partagée entre les exploitants d'installations et les pouvoirs publics. Les notes de posture VIGIPIRATE précisent notamment les catégories de bâtiments devant faire l'objet d'une vigilance ou d'une protection particulière.

Enfin, aux mesures traditionnelles de sécurité des bâtiments, il faut ajouter les procédures, connues de tous, pour permettre la meilleure réaction possible de l'ensemble des personnels en cas d'intrusion malveillante, voire d'attaque terroriste. **La qualité de la préparation d'un établissement conditionne la qualité de sa réaction en cas de crise.**

1.2.2. Préparer un rassemblement[14]

La sécurité d'un événement ne s'improvise pas. Faites-vous conseiller par des professionnels. Pour se préparer à un rassemblement de personnes, il faut :

a) Identifier les menaces et les vulnérabilités

Evaluer la sensibilité du rassemblement en lien avec les services de l'Etat. Pourquoi ce rassemblement pourrait-il être ciblé par des terroristes ? En quoi est-il un symbole du mode de vie occidental et des valeurs de la République ? Ce rassemblement a-t-il une couverture médiatique qui donnerait une forte visibilité à une action terroriste ?

Envisager les différentes attaques possibles : jet ou dépôt d'un engin explosif, véhicule piégé en stationnement aux abords du site, véhicule-bélier, fusillade, attaque à l'arme blanche, etc.

Mettre en place des partenariats avec les acteurs publics locaux :

- **organisez** les relations avec les autorités de police administrative (préfet et maire) afin d'évaluer la menace et les mesures de vigilance et de protection à adopter dans le cadre du rassemblement ;
- **coordonnez-vous** avec les forces de police, gendarmerie, police municipale ou les sapeurs-pompiers.

Si les obligations de sécurité du public ne peuvent être satisfaites ou si les circonstances l'exigent, l'organisateur peut renoncer à la manifestation.

b) Organiser la sécurité de l'événement

La périphérie :

- interdire le stationnement de tout véhicule aux abords immédiats du lieu du rassemblement ;
- mettre en place une signalétique afin d'orienter les piétons sur le lieu de l'événement et de détourner les flux de véhicules ;
- identifier le mobilier urbain qui pourrait servir à dissimuler de l'explosif, l'enlever, en réduire l'utilisation ou mettre en place des rondes de vérification ;
- solliciter les forces de l'ordre ou la police municipale pour la réalisation de patrouilles, voire la mise en place de points de contrôle et de filtrage ;
- identifier les points de vulnérabilité hauts (immeubles surplombants) et les sécuriser, éventuellement par une présence humaine ;
- si possible, mettre en place un système de vidéo-protection donnant, en priorité, sur les accès au site.

La périmétrie :

- installer une délimitation physique de l'événement au moyen de barrières reliées entre elles ;
- organiser un cheminement jusqu'au point de contrôle en installant des barrières ;
- séparer les flux entrants et les flux sortants ;
- aménager, au niveau des accès, des points de contrôle tenus par des agents de sécurité en nombre suffisant afin de fluidifier le plus possible l'entrée du public (l'utilisation de magnétomètres ou de portiques détecteurs de masses métalliques permet d'accroître la qualité des filtrages) ;
- sensibiliser les agents privés de sécurité (consignes de vigilance, etc.) et rappeler par des briefings quotidiens les réactions à adopter en cas d'événement suspect, d'acte de malveillance ou d'attaque terroriste. Les procédures de remontée d'alarme doivent être connues et maîtrisées de tous ;
- doter les agents de sécurité de moyens radio ;
- installer, au niveau des accès publics (entrées et sorties) des dispositifs (blocs de béton, etc.) visant à entraver toute intrusion de véhicule-bélier ;
- contrôler par une présence humaine les points de sortie afin qu'ils ne permettent pas d'intrusion ;
- aménager les issues de secours en nombre suffisant au regard de l'importance de l'événement afin de permettre une évacuation rapide du public en cas de danger à l'intérieur de la zone.

Les volumes intérieurs :

- désigner un responsable sûreté qui sera l'interlocuteur unique des forces de police et de gendarmerie et des secours en cas d'intervention sur le site ;
- faire appel aux compétences de sociétés privées de sécurité pour assurer la sécurité d'un tel événement ;
- sécuriser la zone en période de fermeture au public par la mise en œuvre d'un gardiennage humain ;
- prévoir l'aménagement d'un poste central de sûreté au cœur du site. Ce dernier doit être équipé 24 heures/24 par au moins un opérateur qui visualisera les images du système de vidéo-protection mis en place ;
- sensibiliser les collaborateurs et exposants aux niveaux de menace, aux modes opératoires terroristes et à la détection d'actions de repérage. Cette sensibilisation doit être complétée par une information sur les comportements à adopter en cas d'attaque ;
- installer des écrans et des haut-parleurs pouvant diffuser une alerte (pré-enregistrée si possible) ;
- organiser et contrôler les livraisons.

2. PROTÉGER LES RASSEMBLEMENTS DE MASSE

Description du domaine

Un rassemblement se caractérise par le regroupement public d'un nombre important de personnes dans un lieu ouvert. La protection des rassemblements concerne plusieurs types d'acteurs : **les organisateurs, l'autorité administrative** (maires, préfets), **les forces de l'ordre** (police, gendarmerie, polices municipales).

Les organisateurs sont responsables de la sécurité générale du rassemblement, particulièrement celle des participants. Un service de sécurité propre doit veiller au bon déroulement du rassemblement (filtrage des accès, contrôle des personnes, service d'ordre) et assurer la liaison avec les forces de l'ordre. Il peut être confié au secteur privé.

L'autorité administrative est responsable de l'ordre public. Elle vérifie les mesures prévues par les organisateurs au regard de la nature du rassemblement, de l'importance du public attendu, de la configuration des lieux et des circonstances propres à l'événement. En cas de risque de trouble à l'ordre public ou de menace particulière contre un rassemblement, elle peut l'interdire par un arrêté qu'elle notifie immédiatement aux organisateurs.

Les forces de l'ordre peuvent être engagées sur décision de l'autorité administrative en fonction de la nature ou de la vulnérabilité d'un rassemblement, pour des missions de régulation de circulation, de gestion de foule et de surveillance générale.

Stratégie de sécurité

La stratégie consiste à mettre en place des **dispositifs de surveillance et de contrôle qui s'appuient sur le principe de défense en profondeur.** En dernier recours, il peut être décidé, en fonction de la menace, de limiter, voire d'interdire le rassemblement.

Pour déterminer le niveau de protection d'un rassemblement, il est essentiel d'évaluer la menace à laquelle il est exposé. Une attention particulière doit ainsi être accordée aux rassemblements cumulant forte affluence, renommée touristique et symbole culturel, religieux ou politique. Les notes de posture VIGIPIRATE ont notamment pour objectif d'identifier les catégories de rassemblements les plus sensibles pour une période donnée.