

Guide des **mesures** **de sécurisation** bâtiminaire

Mai 2018

Préambule

La société française est désormais confrontée durablement à une menace terroriste d'un niveau élevé. Elle doit donc se préparer et se protéger.

Ce contexte impose notamment à tous les établissements accueillant du public, d'adopter une démarche permanente de sécurité qui repose principalement sur des mesures simples de vigilance, de prévention et de protection.

Une bonne organisation préalable au sein des immeubles de la DGFIP ainsi qu'une réaction adaptée de l'ensemble des agents peuvent permettre de sauver des vies.

Ce guide de bonnes pratiques, à destination des délégués départementaux à la sécurité, des gestionnaires de site et des agents des services de l'immobilier, présente les mesures de sécurisation périphérique et périmétrique.

Il a pour objectif de fournir des indications simples et précises pour sécuriser a minima les bâtiments et sensibiliser les agents sur les mesures propres à renforcer leur vigilance. En effet, les mesures organisationnelles sont déterminantes pour garantir l'efficacité des moyens techniques existants sur les sites.

Ce guide s'inscrit en amont des guides de bonnes pratiques « Vigilance attentat : les bons réflexes » déclinés pour les cadres et les agents.

Le constat

La taille des bâtiments et leur fréquentation par les usagers sont très variables. Il existe une grande diversité de bâtiments quant à leur situation géographique, leur environnement et leur configuration.

Il en est de même du niveau d'équipement des services en matière de vidéoprotection et de contrôle d'accès.

Dans ce contexte, il appartient à la personne investie du pouvoir de direction, ou à son représentant nommément désigné à cet effet, de veiller à l'adaptation des mesures précisées dans le plan Vigipirate. Il en est de même pour les messages de posture diffusés par le service du Haut fonctionnaire de défense et de sécurité (SHFDS) aux services.

Le préalable : le diagnostic de sûreté

Le diagnostic de sûreté constitue l'étape préalable indispensable à la mise en œuvre cohérente et efficace des mesures de prévention, de vigilance et de protection.

Il est mené par le délégué départemental à la sécurité (DDS), qui dispose du « canevas d'analyse technique de sûreté immobilière » disponible sous Nausicaa.

Il peut être mené, si nécessaire, en partenariat avec le secteur sûreté immobilière (bureau SPiB-2C).

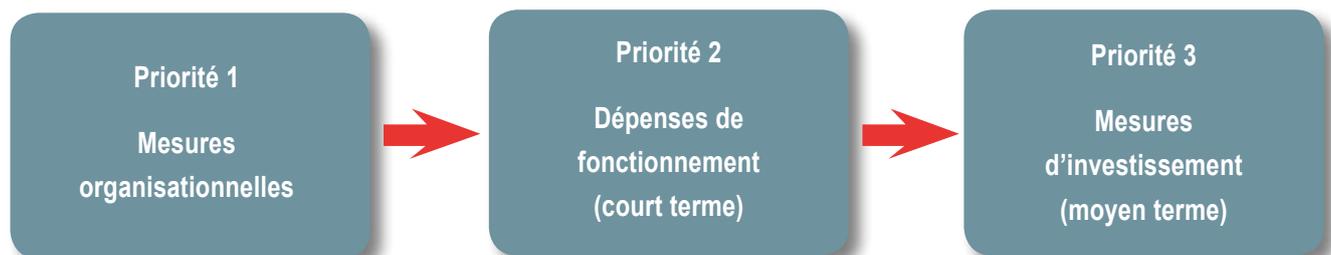
La démarche peut être la suivante :

- ▶ envisager/scénariser les attaques externes et internes :
 - identifier les accès possibles des agresseurs et leurs cheminements ;
 - envisager leurs moyens d'action éventuels (colis ou véhicule piégé, attaque à l'arme blanche, à la voiture bélier, à l'arme automatique...) ;
 - anticiper leurs modes opératoires (ex : le déclenchement de l'alarme incendie pour faire sortir les agents publics et les usagers et faciliter ainsi une atteinte groupée).
- ▶ identifier les vulnérabilités du site (voisinage, abords et emprise du site) ;
- ▶ en déduire les mesures correctives adéquates (limiter le nombre de portes extérieures permettant d'accéder dans le bâtiment pour une meilleure surveillance des flux, sans réduire la capacité d'évacuation du public et des agents, déployer des systèmes de vidéoprotection et de contrôle d'accès adaptés).

Les préconisations concrètes qui en découleront devront être examinées en concertation avec les personnels et leurs représentants syndicaux. Il est en effet primordial que ces mesures soient comprises et acceptées pour être appliquées. Elles pourront également faire apparaître un besoin en formation.

Une démarche pérenne

Dans une logique d'amélioration continue, les mesures de sécurisation doivent être identifiées et mises en place en prenant en compte la priorisation suivante :



Priorité 1 - Les mesures organisationnelles internes au bâtiment nécessitent peu ou pas de dépenses (modification des circulations, organisation de l'accueil au rez-de-chaussée...). Pour la plupart, elles peuvent être mises en œuvre rapidement.

Priorité 2 - En cas de nécessité, il conviendra de recourir aux dépenses de fonctionnement pour faire face à un besoin de sécurisation immédiat. En cas de difficulté, il peut être sollicité un financement dans le cadre du plan urgence sécurité (PUS).

Priorité 3 - Tous les projets de construction ou de réhabilitation doivent intégrer le paramètre sûreté dès leur phase de programmation.

La planification

La sûreté, notamment lorsqu'elle s'appuie sur les préconisations du plan Vigipirate, repose sur des mesures permanentes, dites mesures du socle, ainsi que sur des mesures additionnelles qui traduisent un renforcement progressif de la protection mais aussi des contraintes qui l'accompagnent. Le schéma général en est le suivant :

Surveiller → **Contrôler** → **Limiter** → **Interdire**

Deux dispositifs peuvent grandement faciliter la mise en œuvre des mesures de sûreté : le zonage et le contrôle d'accès.

Le zonage

Le zonage consiste à définir des zones réservées à certaines activités et/ou à certaines personnes ou véhicules (zone de parking réservé aux véhicules des agents, zone d'accueil du public, zone réservée aux rendez-vous avec les usagers, etc.).

Ainsi, il sera recherché conformément à la charte d'aménagement des accueils de 2009, la séparation entre les zones administratives et publiques.

En conséquence, l'usager sera systématiquement pris en charge et raccompagné s'il doit se rendre dans la zone administrative (ce qui doit rester exceptionnel).

Le contrôle d'accès

Le contrôle d'accès consiste à munir les agents et les personnes d'un moyen pour entrer dans le bâtiment :

- une clé (adapté pour les petits sites) ;
- un clavier alphanumérique (dont le code sera changé tous les 6 mois et systématiquement après des travaux) ;
- un badge qui permet d'identifier l'agent. Ce badge peut être permanent (et comporter la photographie et le nom de l'agent) ou temporaire (badge « stagiaire » « prestataire »...). Dans ce dernier cas, il peut être délivré à l'accueil en échange d'une pièce d'identité restituée au visiteur contre le badge lors de son départ. Il est possible de désactiver certains badges à partir d'une heure déterminée.

Dans les grands sites, le badge doit être porté par tous en permanence et de manière apparente.

Certaines zones peuvent être réservées aux seules personnes habilitées. Leur badge sera paramétré en conséquence (ex : le porteur d'un badge « stagiaire » ne pourra pas accéder à tous les services).

La sûreté périphérique

Les mesures de sûreté applicables à l'extérieur de l'emprise du site, sur la voie publique, relèvent de la police de l'ordre public et de la circulation.

Elles ne peuvent donc être décidées et mises en œuvre que par l'autorité détentrice du pouvoir de police administrative, le maire de la commune, le préfet de police de Paris, des Bouches-du-Rhône ou le préfet du département. Les mesures de restriction ou d'interdiction de stationnement des véhicules aux abords des sites devront donc être discutées avec ces autorités.

L'utilisation de la vidéoprotection privée est très encadrée : seuls les accès peuvent être observés, sans vues de la voie publique et des autres bâtiments qui la bordent. Les dispositifs devront respecter les prescriptions de la note de service du 21 septembre 2016 concernant la simplification des démarches relatives à la protection des données personnelles en matière de vidéoprotection.

La vidéoprotection est cependant très utile en matière de protection des sites, tout particulièrement lorsque des agents (écrans de renvoi à positionner dans les bureaux collectifs) peuvent visualiser en temps réel les images, afin de détecter toute menace potentielle et permettre ainsi aux responsables de prendre les mesures appropriées.

Il est toutefois possible de se rapprocher des autorités communales pour envisager une vidéoprotection des abords des bâtiments de la DGFIP par les équipements communaux lorsque la ville en est dotée.

D'une manière générale, il est important que des contacts suivis soient établis avec les municipalités ainsi qu'avec les forces de police ou de gendarmerie.

Ces contacts peuvent permettre d'inclure le site dans les rondes des forces de maintien de l'ordre, de faciliter l'enlèvement des véhicules gênants ou de vérifier des véhicules suspects, etc.

La sûreté périmétrique

La sûreté à l'intérieur de l'emprise de la DGFIP, y compris non bâtie, relève du pouvoir d'organisation du chef d'établissement qui détermine, à partir des préconisations du diagnostic de sûreté et de la déclinaison des mesures Vigipirate, les heures d'ouverture des accès et les catégories de personnes et de véhicules autorisés à les emprunter. Il fixe également les règles de circulation et de stationnement dans le respect des dispositions du Code de la route, notamment en matière de signalisation, et prévoit des restrictions à la circulation et au stationnement.

D'une manière générale, il convient de maintenir fermés les accès surnuméraires ou dont on ne peut pas assurer la surveillance et *a fortiori* le contrôle.

Toutefois, leur condamnation définitive ne doit être envisagée qu'avec prudence et après appréciation de leur utilité en cas de catastrophe importante ou de nécessité d'évacuation d'urgence.

Lorsque c'est possible, il est préférable de distinguer les accès piétons des accès véhicules. Des accès piétons peuvent être réservés aux personnels. Il convient également de réserver un accès aux véhicules de livraison. Un accès et une zone de stationnement particuliers peuvent aussi être réservés aux intervenants de maintenance extérieurs.

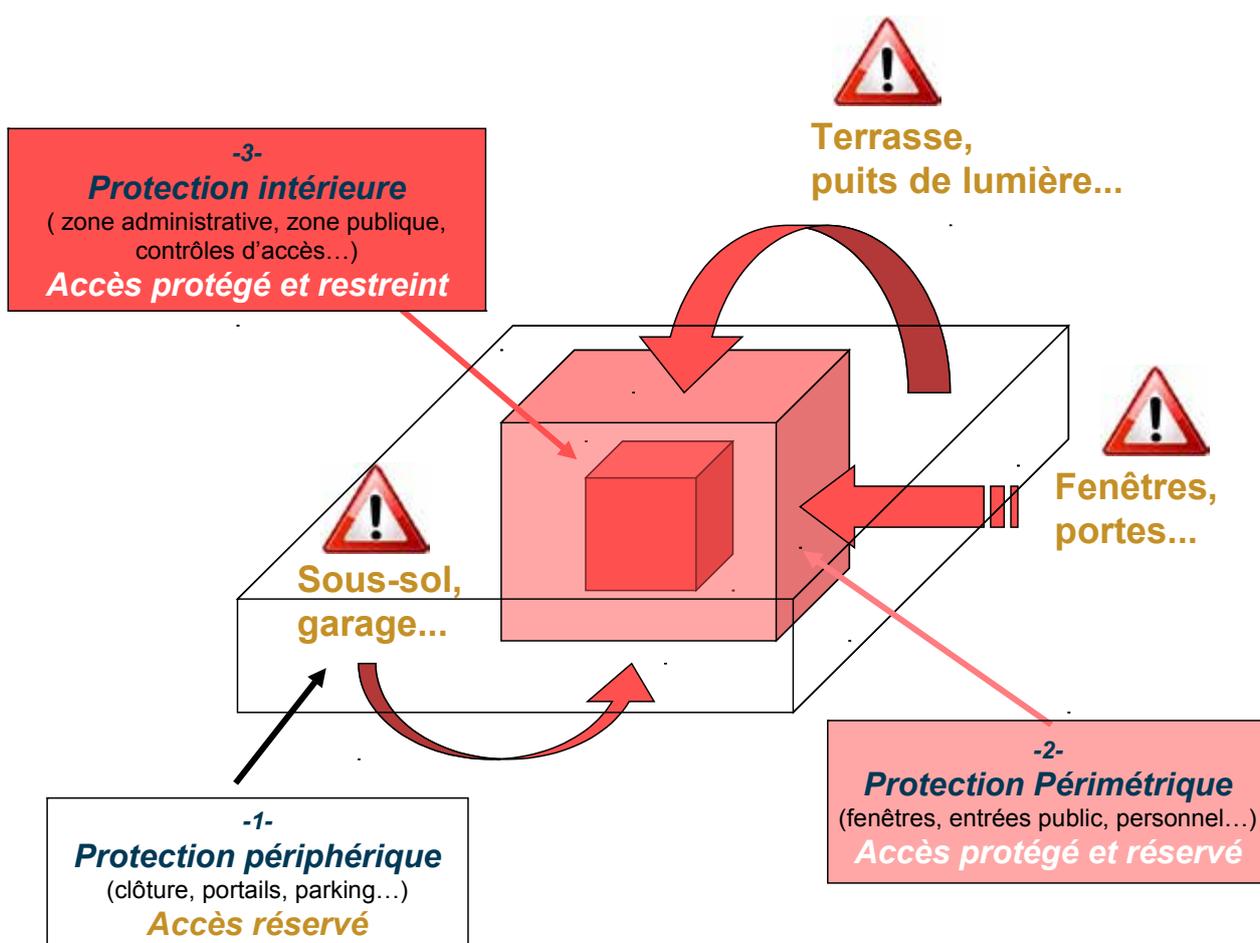
Les parkings doivent, lorsque c'est possible, faire l'objet d'un zonage : personnels, livraisons et maintenance (transport de fonds, le cas échéant...) , usagers.

Moins performante que le contrôle d'accès, l'apposition de vignettes sur le pare-brise des véhicules permet cependant de distinguer ceux qui disposent d'un accès habituel au parking.

Les badges impliquent un dispositif de contrôle d'accès aux différents espaces.

La vignette parking nécessite la présence physique d'au moins une personne aux heures d'accès au parking. Idéalement, il est préférable de disposer d'au moins deux zones de parking séparées : une zone pour le public et une zone pour le personnel sur laquelle sera mise en place un contrôle d'accès à partir de badges (les mêmes que ceux pour accéder dans les services).

Il faudra également veiller à ce que les contrôles d'accès des véhicules et des piétons ne génèrent pas d'embouteillage ou de file d'attente sur la voie publique.



La sûreté bâtiminaire

La sûreté bâtiminaire repose en grande partie sur le contrôle des accès et le zonage.

Une fois encore, il est nécessaire de verrouiller les accès inutiles tout en maintenant les issues de secours fonctionnelles (à vérifier périodiquement).

Afin que les issues de secours ne restent pas ouvertes, des «zones fumeurs» devront être prévues.

D'une manière générale, qu'il s'agisse d'accès de secours maintenus ouverts ou de l'utilisation d'accès réservés comme «raccourcis», les détournements d'usage doivent être strictement interdits. Ces comportements nuisent gravement à la sûreté des sites.

Idéalement, sur les petites et moyennes structures, l'accueil doit disposer d'un dispositif de télécommande de l'ouverture de la porte ou du sas de l'entrée principale et d'une vue directe sur les personnes demandant l'accès. A défaut, un vidéo-portier ou un écran de report de vidéoprotection sera installé. Sur les grands sites, où les flux ne permettent pas de maintenir l'accès visiteurs fermé, il convient de prévoir un dispositif de condamnation des portes d'accès principal en cas de besoin (ex : manifestations sociales...).

L'information des forces de l'ordre en cas d'incident grave est effectué soit directement par un appel téléphonique (urgence 17) soit par le dispositif d'alarme relié au télésurveilleur national de la DGFiP.

De même, il convient de mettre en place un système d'alerte connu de tous, par exemple une alerte sonore spécifique, **distincte de l'alarme incendie**, (message par haut-parleur, sifflet, corne de brume...). L'alerte doit permettre de prévenir, au plus vite, l'ensemble du site d'une attaque.

La plus grande vigilance face aux lettres et colis devra être recommandée aux services « courrier ». Les colis apportés par des coursiers devront être enregistrés et les destinataires contactés par l'accueil afin qu'ils en prennent eux-mêmes livraison, ce qui permet d'en assurer la traçabilité et de vérifier qu'ils correspondent bien à une commande ou à un envoi attendu. Il est par ailleurs à noter que le courrier et les colis doivent être ouverts dans des locaux non ventilés.

Lorsque cela s'avère possible, il convient de privilégier l'accueil des usagers sur rendez-vous. Un zonage adéquat peut alors être mis en œuvre.

L'accompagnement des visiteurs au-delà de la zone d'accueil doit être systématique, depuis leur arrivée jusqu'à leur départ.

Les personnels d'accueil doivent détenir la liste des personnes extérieures à l'établissement conviées à participer à une réunion.

Ils peuvent demander aux visiteurs leur pièce d'identité et noter leur nom, heures d'arrivée et de départ, sur une main courante.

Enfin, il peut être judicieux d'étudier la possibilité de «sanctuariser» certains locaux afin de pouvoir y mettre à l'abri les agents, voire le public présent, en cas d'attaque terroriste lorsque ceux-ci ne sont pas en mesure de s'échapper sans danger.

Dans chaque site, la rédaction d'un « règlement intérieur de sûreté » détaillant l'ensemble des procédures de sûreté à mettre en œuvre est préconisée. Ce document, mis à jour régulièrement, est porté à la connaissance de tout nouvel agent affecté sur le site qui s'engage à en respecter les termes.

Il peut faire l'objet de réunions d'information générales ou spécifiques afin de sensibiliser les agents aux bonnes pratiques en la matière.

La formation des personnels

Il est nécessaire de former des personnels de direction et d'encadrement aux problématiques de sécurité et l'ensemble des agents à la vigilance.

Des exercices peuvent être organisés afin de préparer les agents à réagir en cas d'incident grave. Les exercices proposés sont progressifs (cf. documents joints en annexe).

L'acculturation sécuritaire

Le gestionnaire de site et le délégué départemental à la sécurité doivent être clairement identifiés par les agents et facilement joignables.

L'information et la communication, régulièrement réitérées, sont essentielles pour obtenir l'adhésion des agents à la politique de mise en sûreté du site, l'appropriation de comportements responsables (fermeture des portes, regroupement des objets à détruire, des poubelles, dans les lieux prévus à cet effet, etc.) ainsi que leur collaboration dans la détection des situations anormales (dysfonctionnement d'équipements de sécurité, véhicules, individus ou colis suspects, radicalisation de collègues, etc.).

Leur sûreté et au-delà, celle des usagers, dépend avant tout d'eux-mêmes. La sûreté est l'affaire de tous, a fortiori quand on envisage les risques les plus graves. Au final, **la sûreté dépendra d'abord et surtout de mesures humaines et organisationnelles** puis dans un second temps de dispositifs techniques.

La clé principale est la sensibilisation des agents

▶ **Sensibiliser les agents** aux mesures de sûreté et de vigilance élémentaire (filtrage des accès, surveillance de la circulation interne dans les bâtiments, sécurisation des déplacements et des locaux) ;

▶ **Se préparer :**

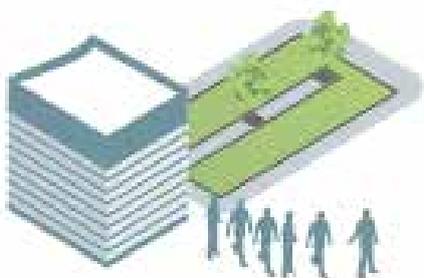
1. rappeler les procédures et le rôle de chacun ;
2. s'assurer de la connaissance par tous des moyens d'alerte ;
3. réaliser des exercices simples de mise en situation ;
4. réaliser des exercices complets intégrant éventuellement les différents partenaires ;
5. exploiter systématiquement les retours d'expérience.

▶ **Se former** aux premiers secours

<http://www.gouvernement.fr/risques/se-former-aux-premiers-secours>

Les exercices
doivent être
réguliers
et progressifs

Bien connaître son environnement quotidien



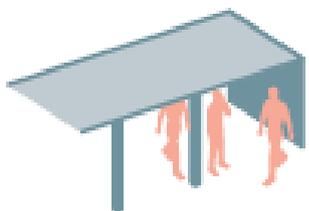
- ▶ **Connaître la configuration du site** (agencement des bâtiments, aménagement des espaces) en organisant des « reconnaissances exploratoires » : identifier les cheminements, issues de secours, obstacles éventuels, tout ce qui peut offrir une protection, etc ;



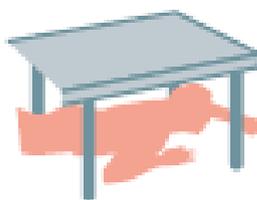
- ▶ **Savoir auprès de qui signaler** les comportements et situations inhabituels ;



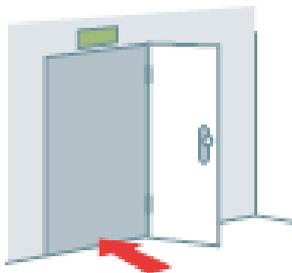
- ▶ **Connaître les moyens d'alerte** propres au site ;



- ▶ **Identifier les lieux de confinement et où se cacher** éventuellement ;



- ▶ **Identifier le mobilier utile et disponible pour se barricader** et se protéger ;



- ▶ **Vérifier régulièrement** la disponibilité et la vacuité des issues de secours ;

- ▶ **Connaître son environnement extérieur** : emprise du site, voisinage

L'information et la sensibilisation des agents sont faites par la personne désignée à cet effet

Développer la vigilance



- ▶ **Encourager la vigilance des agents** afin de détecter et signaler les comportements suspects et les situations inhabituelles :
 - sac abandonné, colis suspect ;
 - véhicule suspect (stationnement prolongé, comportement des occupants, moteur tournant) ;
 - attitude laissant supposer un repérage (allées et venues, observation prolongée, etc.) ;
 - sous-traitants, livreurs en dehors de leur zone et horaires d'intervention.



- ▶ **Faire remonter**, suivant la procédure établie, **toute situation particulière** (menaces verbales, tags menaçants, appels téléphoniques anonymes, etc.).



- ▶ **Signaler tout changement de comportement** chez un agent ou un usager du service (signes de radicalisation).

« Ce n'est
probablement
rien mais... »

S'informer, se former, s'exercer sont les clés d'une bonne préparation

Le présent guide ne prétend pas à l'exhaustivité des mesures organisationnelles ou concrètes qui pourraient être mise en œuvre pour sécuriser un bâtiment, voire ralentir une attaque terroriste et en réduire l'impact, si elles ne suffisent pas à l'empêcher. Il constitue une aide à la réflexion en formulant des pistes de recherche de solutions de sécurisation, variables selon le type d'immeuble à protéger et du public qu'il accueille.

Les mesures arrêtées devront être régulièrement testées à l'occasion d'exercices qui permettront à la fois de vérifier la résilience des personnels et leur appropriation de ces mesures.

Les bonnes pratiques



► Identifier le délégué départemental à la sécurité (DDS)

Interlocuteur :

- de la référente sûreté immobilière et du commissaire divisionnaire de police du bureau SPiB 2C, et le cas échéant du référent sûreté local de la police ou de la gendarmerie,
- des personnels.



► Établir des contacts suivis avec la municipalité et les forces de police ou de gendarmerie.



► Établir un diagnostic de sûreté du bâtiment et de son emprise.



► Faire respecter les mesures organisationnelles, surveiller ► contrôler ► limiter ► interdire



► Budgétiser les mesures de protection techniques.

Les bonnes pratiques



► **Créer des zones dans les emprises, les parkings et les bâtiments**

Définir qui (personnes, véhicules) a accès aux différentes zones et quand. Fixer dans le règlement intérieur les règles de circulation et de stationnement et prévoir une graduation, par exemple par zonage ou par catégorie, des restrictions à la circulation et au stationnement.



► **Instaurer un système de contrôle d'accès**



► **Demander aux autorités de police administratives compétentes** d'instaurer les mesures de protection extérieures nécessaires : interdictions de stationner, de circuler, rondes, vidéoprotection des abords.



► **Faire modifier ou remplacer les poubelles publiques** (supports de sacs transparents)



► **Installer un système de vidéoprotection** avec renvoi dans un bureau collectif.

Les bonnes pratiques

- ▶ **Maintenir fermés les accès surnuméraires** ou dont on ne peut pas assurer la surveillance ou le contrôle, les issues de secours restant fonctionnelles. Interdire strictement les «détournements d'usage» des accès.



- ▶ **Garantir l'étanchéité** entre la zone publique et la zone administrative.



- ▶ **Munir l'accueil d'un dispositif de télécommande** de l'ouverture de la porte ou du sas de l'accès principal. À défaut, prévoir un dispositif de condamnation des portes d'accès principal.



- ▶ **Privilégier l'accueil des usagers** au rez-de-chaussée et/ou sur rendez-vous.



- ▶ **Être très vigilants** face aux lettres et colis.

Les bonnes pratiques



- ▶ **Munir les personnels d'accueil** de la liste des personnes conviées à participer à une réunion.



- ▶ **Demander aux visiteurs de produire une pièce d'identité**, noter leur nom, heures d'arrivée et de départ, sur une main courante et les accompagner systématiquement.



- ▶ « **Sanctuariser** » certains locaux afin de pouvoir y mettre à l'abri les agents et les usagers en cas d'attaque terroriste.



- ▶ **Former des personnels de direction et d'encadrement** aux problématiques de sécurité et l'ensemble des personnels à la vigilance.

Ce document a été réalisé par la



en collaboration avec



Secrétariat général
de la défense
et de la sécurité nationale

