RECOMMANDATIONS POUR LA SÉCURISATION DES LIEUX DE RASSEMBLEMENT OUVERTS AU PUBLIC

(Fiche actualisée en date du 2 novembre 2017)

Cette fiche traite de la protection des lieux de rassemblement ouverts au public (événements sportifs, festivals, marchés de Noël, braderies, etc.) et doit pouvoir servir de guide pratique aux organisateurs de ce genre de manifestations. Elle doit être largement diffusée. Certains des conseils délivrés ci-dessous peuvent ne pas être applicables à tous les sites. Ils doivent donc être adaptés en fonction de la configuration des lieux et du bon sens de circonstance.

1 Identifier les menaces et les vulnérabilités

Il faut d'abord évaluer la sensibilité du rassemblement en lien avec les autorités locales (préfet, maire, Police Nationale, Gendarmerie Nationale) :

- 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 ?

Les différentes attaques possibles doivent être envisagées :

- jet ou dépôt d'un engin explosif à l'intérieur ou en périmétrie du site ;
- véhicule piégé en stationnement aux abords du site ;
- véhicule-bélier ;
- fusillade ou attaque suicide ;
- prise d'otage ;
- attaque à l'arme blanche.

2 Organiser la sécurité de l'événement

Il est primordial que les organisateurs de rassemblements se coordonnent avec le maire et le préfet, ainsi qu'avec les forces de police, de gendarmerie, les services de police municipale et d'incendie et de secours.

Par ailleurs, il peut être nécessaire de faire appel aux compétences de sociétés privées de sécurité pour renforcer la sécurité d'un tel événement.

2.1 - En périphérie du rassemblement

- **choisir le lieu d'implantation de l'événement qui présentera le moins de vulnérabilités.** Il est préférable de choisir le lieu du rassemblement de manière à limiter l'accès de véhicules (ne pas s'installer au débouché d'un axe important) ;
- **limiter ou interdire le stationnement** des véhicules 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 ;
- **cloisonner le flux des véhicules de l'espace de déambulation des piétons ;**
- **identifier le mobilier urbain** qui pourrait servir à dissimuler de l'explosif, le faire retirer par les autorités habilitées, 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. Des agents des sociétés privées de sécurité peuvent concourir à cette mission ;
- **identifier les points de vulnérabilité hauts** (immeubles surplombant) et les sécuriser, éventuellement par une présence humaine ;
- si possible, mettre en place un système de vidéoprotection donnant, en priorité, sur les accès au site, en prenant en compte les dispositions du Code de la sécurité intérieure.

2.2 - Sur la périmétrie du rassemblement

- **aménager des points de contrôle ou de filtrage en nombre suffisant** aux entrées du site afin de fluidifier l'entrée du public. Leur efficacité repose sur la présence d'un superviseur, de moyens de communication et de procédures claires afin de diffuser l'alerte et de faciliter l'intervention des forces de sécurité intérieure en cas d'incident ;
- **maintenir le niveau de vigilance tout au long de l'événement mais également lors du moment sensible de sa dispersion** (le 22 mai 2017 à Manchester, au Royaume-Uni, un homme a fait détoner une charge explosive qu'il portait sur lui à la sortie de la salle de spectacle *Manchester Arena*), en rappelant régulièrement des messages de sensibilisation à destination du public (*via* la sonorisation de l'événement par exemple – « TOUS acteurs de la sécurité) » ;
- **installer une délimitation physique du périmètre extérieur** de l'événement au moyen de barrières reliées entre elles, de blocs en béton, de véhicules du comité d'organisation comme élément de barrage, etc. ;
- organiser un ou plusieurs cheminements jusqu'au point de contrôle en installant des barrières. Séparer, dans la mesure du possible, les flux entrants et les flux sortants ;
- **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 ;
- **organiser et contrôler les livraisons.** Prévoir des équipements mobiles permettant de bloquer physiquement les véhicules appelés à pénétrer dans le périmètre le temps de ce contrôle ;
- apposer les affiches de sensibilisation à destination du public aux points d'entrées notamment « Réagir en cas d'attaque terroriste ».

Les véhicules-béliers constituent un mode d'action terroriste de plus en plus utilisé : attentats de Nice et de Berlin en 2016, attaque contre une patrouille de militaires à Levallois-Perret et attentats en Catalogne en 2017.
Il est recommandé de mettre en place des moyens de circonstance permettant d'interdire l'accès au site ou de réduire la vitesse des véhicules à proximité des lieux de rassemblement. La mise en place de chicanes avec des obstacles successifs est également conseillée : plots en béton, bacs de fleurs de dimensions importantes, herses mobiles, barrières d'arrêt ou véhicules lourds (camions). Il est indispensable de tenir compte de la distance de pénétration potentielle d'un véhicule-bélier lors de la définition du périmètre extérieur d'un rassemblement (distance de sécurité entre les dispositifs de sécurité et la foule).

Exemple de revue de propagande de l'Etat Islamique qui préconise le recours à un véhicule-bélier.

2.3 - Au niveau des volumes intérieurs

- **désigner un responsable sûreté** qui sera l'interlocuteur unique des forces de l'ordre et des services d'incendie et de secours en cas d'intervention sur le site. Véritable coordinateur de la sûreté de l'événement, il doit connaître les bons réflexes à adopter. Il peut se rapprocher préalablement des forces de sécurité intérieure pour recueillir leurs conseils ;
- prévoir l'aménagement d'un **poste central de sûreté** au sein du site. Ce dernier doit être équipé 24H/24 par au moins un opérateur en mesure de visualiser les images du système de vidéo-protection mis en place ;
- **sécuriser la zone en période de fermeture du public** par la mise en œuvre d'un gardiennage humain ;
- **sensibiliser l'ensemble des collaborateurs au niveau de menace,** aux modes opératoires terroristes et à la détection de situations suspectes. Cette sensibilisation doit être complétée par une information sur les comportements à adopter en cas d'attaque.

SGDSN
SECRÉTARIAT GÉNÉRAL
DE LA DÉFENSE ET DE
LA SÉCURITÉ NATIONALE

51, boulevard de La Tour-Maubourg
75700 Paris SP 07
01 71 75 80 11
sgdsn.gouv.fr

Maquette et impression : Pôle Conception graphique-Fabrication – DSAF/DPL – Octobre 2017.

VIGIPIRATE

ORGANISER UN CONFINEMENT FACE À UNE MENACE TERRORISTE

Fiche pratique à destination des responsables d'établissement accueillant du public.

Pour garantir au mieux la sécurité des personnes, les établissements accueillant du public devront mener une réflexion sur la question du confinement, de la décision à la levée de celle-ci.

Cette fiche pratique à destination des responsables de sécurité et de sûreté de ces établissements dispense des recommandations et des bonnes pratiques à adopter pour se préparer face à la menace terroriste.

En cas d'attaque armée, il est nécessaire de déterminer la réponse la plus appropriée à la situation. Celle-ci n'est pas figée, elle évolue : adoptez vos modes de réaction aux circonstances.

Le confinement est envisageable **si l'attaque est extérieure** au site dans lequel vous vous trouvez ou **si l'attaque survient à l'intérieur** mais que s'échapper semble trop dangereux.

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

1 Comment se préparer ?

Pour limiter les risques et les dangers que peut entraîner le confinement, certaines recommandations, tirées de plusieurs confinement réels en 2017, permettent de se préparer et d'anticiper les situations d'urgence :

- **Elaborer un plan de mise en sûreté** prévoyant :
  - les missions des personnels ;
  - les zones possibles de confinement ;
  - les coordonnées des forces de sécurité intérieure les plus proches ;
  - Les missions de chacun suivant les périodes de l'année (jours fériés, horaires atypiques, vacances scolaires, etc.) ;
  - la reprise de l'activité normale.
- **S'appuyer sur un poste central de sûreté ou un moyen de centraliser l'information,** suivant la taille de l'établissement et désigner un responsable.
- **Identifier les personnels de confiance** qui peuvent seconder le responsable de l'établissement pour accueillir, sécuriser et rassurer le public présent sur le site.
- **Informer et sensibiliser** les personnels plusieurs fois dans l'année.
- **Organiser des exercices,** à différentes périodes de l'année au sein de l'établissement (week-end, personnel réduit, etc.) afin d'identifier les vulnérabilités.
- **Identifier plusieurs zones de confinement,** mécaniquement sanctuarisables, si possible avec un point d'eau et des toilettes et dont l'accès est exclusivement réservé aux acteurs gestionnaires du risque.
- **Envisager les difficultés potentielles de communication** avec le public et s'y préparer (langage corporel, etc.).

L'organisation de la coordination est fondamentale

- **Etablir et conserver un contact permanent** entre un responsable identifié au sein du site et les forces de sécurité intérieure.
- **Mettre en place des moyens de communication interne** entre les différentes zones de l'établissement (radios, logiciels internes, etc.).
- **Rendre accessibles les moyens de transmission aux forces de sécurité intérieure** (moyens radios mobiles supplémentaires, report de vidéoprotection, etc.).
- **Préenregistrer un message d'alerte le moins anxiogène possible.**

ORGANISER UN CONFINEMENT FACE À UNE MENACE TERRORISTE

FICHE PRATIQUE À DESTINATION DES RESPONSABLES D'ÉTABLISSEMENT ACCUEILLANT DU PUBLIC.

2 Comment organiser un confinement ?

2.1 - Décider du confinement

a) Qui décide ?

La décision de confinement relève du bon sens. Elle est prise le plus souvent par le responsable de l'établissement mais peut également l'être par l'ensemble des personnels directement au contact d'une situation l'exigeant. Elle peut être prise par l'ensemble des personnels.

Les personnels doivent être sensibilisés aux procédures prévues dans leur établissement.

b) Comment le mettre en place ?

Diffuser un message à l'attention du public en utilisant un ton non-anxiogène. L'objectif est d'éviter à tout prix de déclencher une panique. Il est conseillé de préenregistrer un message.

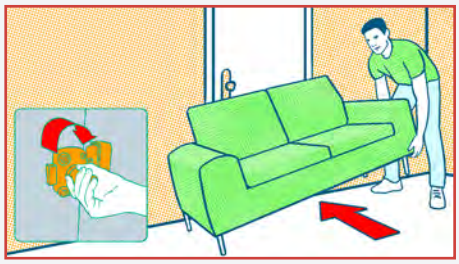
Envisager l'installation d'un système de sonorisation dans tout ou partie de l'établissement.

Prévoir un système d'appel automatique sur les postes fixes avec un message pré-enregistré et/ou envoi de SMS aux personnels.

2.2 - Gérer le confinement

Suivant le niveau de menace connu ou ressenti, il est possible de prendre certaines dispositions :

- bloquer les portes avec des moyens de fortune ;
- éteindre les lumières ;
- s'éloigner des portes et fenêtres ;
- s'allonger au sol ;
- faire respecter le silence (mode silence des téléphones).



Une fois à l'abri, prévenez les forces de sécurité en donnant les informations essentielles (où, quoi, qui, combien, comment).

Tenir informées du mieux possible les forces de sécurité intérieure sur les conditions du confinement.

Prévenez ou faites prévenir les sites voisins.

Travailler sur l'attitude rassurante des personnels. Oser répéter les informations et **communiquer régulièrement** avec le public. Informer sur un point d'eau ou des toilettes éventuelles dans la zone de confinement.

Recommander aux personnes de rassurer leur entourage par message, plutôt que par conversation téléphonique (risque de saturation), et d'éviter de diffuser sur les réseaux sociaux des informations en temps réel.

Rester vigilant sur les comportements anormaux (stress extrême, comportement agressif ou suspect).

2.3 - Lever le confinement

Attendre l'autorisation des forces de sécurité intérieure pour lever le confinement.

Maintenir un encadrement rigoureux de la foule pour assurer une dispersion fluide lors de son évacuation.

Guider le public dans la direction de l'évacuation en fonction des consignes données par les autorités.

SGDSN
SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

51, boulevard de La Tour-Maubourg
75700 Paris SP 07
01 71 75 80 11
sgdsn.gouv.fr

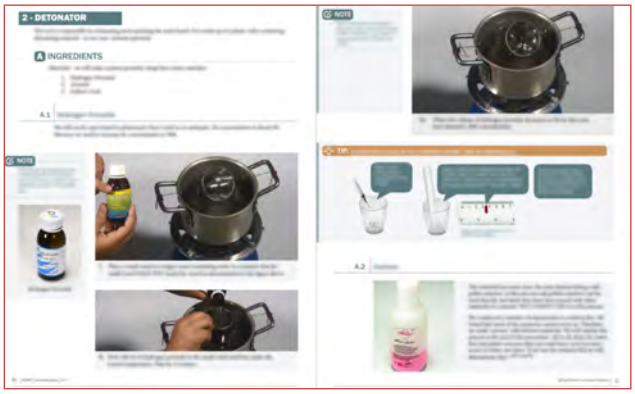
Maquette et impression : Pôle Conception graphique-Fabrication – DSAF/DPL – Juillet 2017.

PRODUITS CHIMIQUES :
SIGNALEMENT DE TOUT VOL OU UTILISATION SUSPECTE

Les derniers attentats ou actes de malveillance commis en Europe ont montré la capacité des criminels et terroristes à fabriquer des explosifs artisanaux ou des substances toxiques en utilisant des produits chimiques d'usage courant, souvent disponibles dans les magasins de bricolage, les jardineries, les grandes surfaces, etc.

Des tentatives d'attentats ont pu être déjouées grâce aux signalements de comportements ou d'achats suspects de produits chimiques (engrais, solutions de nettoyage de piscine, détachant, dissolvant, etc.).

- Novembre 2015 : **attentats de Paris** (stade de France, Bataclan) ;
- Mars 2016 : **attentats à l'aéroport de Bruxelles-Zaventen** et à la **station Maelbeek** (Belgique) ;
- Février 2017 : découverte d'un laboratoire de fabrication d'explosifs à **Montpellier** – attentat déjoué ;
- Avril 2017 : découverte d'un laboratoire de fabrication d'explosifs à **Marseille** – attentat déjoué ;
- Mai 2017 : **attentat de Manchester** (Royaume-Uni) ;
- Août 2017 : explosion d'un laboratoire de fabrication d'explosifs à **Alcanar** (Espagne) ;
- Eté 2017 : jets d'acide à **Londres** (Royaume-Uni) ;
- Août 2017: découverte d'un projet d'engin chimique à **Sidney** (Australie) ;
- Septembre 2017 : jet d'acide à **Marseille** ;
- Septembre 2017: découverte d'un **laboratoire clandestin** de fabrication d'explosifs à **Villejuif.**



Des recettes disponibles sur Internet

Un laboratoire de fabrication d'explosifs artisanaux

1 Comment détecter une utilisation suspecte de produits chimiques ?

En étant attentif à son environnement, chacun **peut détecter** la fabrication de substances permettant de commettre des attentats. Les éléments suivants, **constatés dans un lieu inapproprié, doivent vous alerter :**

- divers **produits chimiques** en quantité inhabituelle ;
- des **équipements** tels que des moyens de chauffage, des ustensiles de cuisine ou de la verrerie de laboratoire, des gants et lunettes de protection ;
- une **odeur** suspecte.

SUBSTANCES CHIMIQUES + MATÉRIELS INAPROPRIÉS (+ ODEURS) = SIGNALEMENT

2 Comment réagir et signaler ?

Si vous êtes témoin d'une utilisation suspecte de produits chimiques, **ne vous mettez pas en danger, restez discret et appelez sans délai les forces de sécurité intérieure** en composant le 17, 112 ou 114 (pour les personnes ayant des difficultés à entendre et à parler).

3 Quelles sont les obligations des professionnels qui commercialisent des produits chimiques ?

La réglementation française (*décret n°2017-1308 du 29 août 2017*) prévoit des mesures pour restreindre l'accès du grand public à des substances chimiques d'usage courant :

	Présence possible dans…	INTERDICTION de vendre aux particuliers (au delà d'une certaine concentration)	Autorisation de vendre aux particuliers avec obligation d'ENREGISTREMENT par le vendeur	SIGNALEMENT au point de contact national (PIXAF) de tout vol, perte, disparition ou transaction suspecte
Peroxyde d'hydrogène (7722-84-1)	Produits de blanchissage, décolorants capillaires, désinfectants, agents nettoyants	> 35% p/p	de 12 < % p/p ≤ 35	
Nitrométhane (75-52-5)	Carburants pour modèles réduits, solvants	> 40% p/p	de 30 < % p/p ≤ 40	
Acide nitrique (7697-37-2)	Décapants, traitement des métaux	> 10% p/p	de 3 < % p/p ≤ 10	
Chlorate de sodium (7775-09-9), **chlorate de potassium** (3811-04-9), **perchlorate de sodium** (7601-89-0) et **perchlorate de potassium** (77778-74-7)	Articles pyrotechniques	> 40% p/p		
Nitrate d'ammonium (6484-52-2)	Engrais, poche de froid			
Acétone (67-64-1)	Dissolvants, solvants			
Hexamine (100-97-0)	Additifs alimentaires, carburants solides pour réchauds de camping et pour moteurs à vapeur de modèles réduits			
Acide sulfurique (7664-93-9)	Déboucheurs de canalisation			
Nitrate de potassium (7757-79-1), **nitrate de sodium** (7631-99-4)	Engrais, conservateurs alimentaires			
Poudres d'aluminium (7429-90-5) et de **magnésium** (7439-95-4) **Nitrate de calcium** (10124-37-5) **Nitrate de magnésium hexahydraté** (13446-18-9)	Engrais			

Pour plus de détails, contacter le service central des armes (ministère de l'intérieur/SCA) :
sca-precurseurs-explosifs@interieur.gouv.fr

Quels critères permettent de détecter une transaction suspecte de produits chimiques à des fins malveillantes ?

Les critères suivants peuvent alerter un professionnel :

- absence d'explications cohérentes sur l'utilisation prévue des produits ;
- utilisation du produit inconnue de l'acheteur ;
- réticence à dévoiler l'utilisation du produit ;
- quantités, combinaisons ou concentrations inhabituelles de produits pour un usage domestique ;
- réticence de l'acheteur à donner les éléments nécessaires à l'enregistrement de la transaction ;
- paiement important en espèces ;
- tentative de communiquer le moins possible ;
- refus de tout produit de substitution ou de plus faible concentration.

Que faire en cas de vol, disparition ou transaction suspecte de produits chimiques réglementés ?

Les professionnels ont l'obligation de signaler tout vol, disparition ou transaction suspects au **point de contact national :**

Plateau d'Investigation eXplosifs et Armes à Feu de la Gendarmerie nationale
pixaf@gendarmerie.interieur.gouv.fr - 01 78 47 34 29 (24H/24H)

VOL ou DISPARITION ou TRANSACTION SUSPECTE = SIGNALEMENT

SGDSN
SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

51, boulevard de La Tour-Maubourg
75700 Paris SP 07
01 71 75 80 11
sgdsn.gouv.fr

Maquette et impression : Pôle Conception graphique-Fabrication – DSAF/DPL – Octobre 2017.

VIGIPIRATE

SÉCURITÉ DU NUMÉRIQUE
L'HAMEÇONNAGE (OU PHISHING)

Cible : personnels des organismes privés et publics

1 Et si c'était vous ?

Ingénierie sociale

Alors que vous assurez la permanence pendant les fêtes de fin d'année, un individu vous contacte par téléphone. Il souhaite obtenir rapidement, pour motif professionnel, les codes d'accès de l'application financière en charge des paiements fournisseurs et des salaires. À force d'arguments et grâce à un ton assuré, il réussit à vous convaincre et, en l'absence de votre hiérarchie, vous cédez sous la pression et lui communiquez l'information convoitée.

S'il ne s'agit pas d'une attaque informatique directe mais d'une technique répandue d'ingénierie sociale, ce type d'information (code d'accès, coordonnées bancaires, données personnelles, etc.) peut être utilisé comme point d'entrée pour mener une attaque à l'encontre de votre organisme.

Attaque par la messagerie

Au retour d'une absence prolongée du bureau, vous trouvez votre messagerie électronique engorgée. Pressé, vous ignorez l'invitation à redémarrer votre ordinateur et empêchez par conséquent l'installation des mises à jour. En parcourant rapidement les objets de vos courriels, l'un d'eux semble traiter d'affaires en cours vous concernant directement et retient votre attention. Vous l'ouvrez et y découvrez un bref message vous enjoignant de consulter un site Internet qui vous est familier dans l'exercice quotidien de vos fonctions.

Vous venez d'être victime d'hameçonnage (ou *phishing*).

En contrevenant à un principe d'hygiène fondamental (mettre à jour ses logiciels) et en cliquant sur ce lien d'apparence légitime sans prêter attention à certains détails, vous avez permis à un attaquant d'installer un programme malveillant dans le système d'information de votre entreprise et vous lui avez donné accès non seulement à vos dossiers mais aussi à ceux de vos collègues.

2 Comment renforcer ma vigilance et bien me protéger ?

Qu'est-ce que l'hameçonnage ?

L'hameçonnage est une technique d'attaque prenant la forme d'un courriel qui vous est adressé et qui semble provenir d'un expéditeur de confiance. Ce courriel peut contenir un **fichier**, une **pièce jointe** ou un **lien de redirection vers un site frauduleux**, avec une incitation à cliquer sur ces éléments, ce qui permettra à l'attaquant de recueillir de l'information ou d'installer un programme malveillant dans le système d'information de votre organisme.

Adopter les bonnes pratiques au quotidien

- Méfiez-vous des courriels exigeant de vous une réponse ou une action immédiate et vous intimant de ne pas en informer votre hiérarchie ou vos collaborateurs.
- Soyez prudents vis-à-vis des courriels comportant des visuels a priori officiels mais dont la résolution est mauvaise.
- Ne cliquez jamais sur un lien ou une pièce jointe dont l'origine ou la nature vous semblent douteuses. **Au moindre doute, privilégiez l'accès au site web en tapant directement l'adresse** dans la barre de recherche.
- Soyez à l'affût des fautes d'orthographe ou de syntaxe dans l'adresse de l'expéditeur, l'objet du courriel ou le corps du texte.
- Ne répondez jamais à un courriel vous demandant des informations confidentielles (identifiants, coordonnées bancaires, etc.). **Au moindre doute, n'hésitez pas à contacter l'expéditeur** par un autre canal, par exemple téléphonique.
- Méfiez-vous des courriels d'expéditeur connu mais dont l'adresse électronique ou la nature du message sont inhabituelles ou catégorisés comme « spam / indésirable » par le logiciel de messagerie.
- Procédez régulièrement au redémarrage de votre poste, notamment lorsque le système vous y invite.

3 Je pense avoir été victime d'une attaque. Que faire ?

Qui prévenir ?

Si vous pensez avoir été victime d'une attaque informatique :

- prévenez immédiatement le support informatique de votre organisme et vos supérieurs hiérarchiques ;
- procédez sans délai au renouvellement de vos identifiants si vous les avez transmis lors de l'attaque.

4 Documents de référence

Guide des bonnes pratiques de l'informatique
http://www.ssi.gouv.fr/uploads/2017/01/guide_cpme_bonnes_pratiques.pdf

SGDSN
SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

51, boulevard de La Tour-Maubourg
75700 Paris SP 07
01 71 75 80 11
sgdsn.gouv.fr

Maquette et impression : Pôle Conception graphique-Fabrication – DSAF/DPL – Octobre 2017.

POSTURE « TRANSITION 2017-2018 »

MESURES PUBLIQUES (1/5)

Action	Libellé mesure	Commentaires	N° mesure
	Diffuser l'alerte au grand public	**Activation des cellules de veille et de crise laissée à 'appréciation des autorités académiques ou des établissement d'enseignement supérieur et de recherche** **RAPPEL** - Afficher le logo du niveau ***« sécurité renforcée-risque attentat »*** à l'entrée des sites accueillant du public.  Ces logos doivent être affichés à l'entrée et dans les espaces d'attentes des sites accueillant du public et peuvent être complétés d'une fiche synthétique récapitulant les conditions particulières de sécurité au sein de la structure. L'utilisation du logo ***« urgence attentat »*** fera l'objet d'instructions particulières en cas d'activation de ce niveau.  - Encourager et organiser la remontée des signes pouvant précéder une crise ou un attentat : comportements anormaux de personnes ou de véhicules, repérages, bagages ou colis abandonnés, etc. - Recommander le téléchargement de l'application pour Smartphone "Système d'alerte et d'information des populations" (SAIP) : http://www.gouvernement.fr/appli-alerte-saip	ALR 11-02 ALR 11-04

Sensibiliser Informer Alerter	Sensibiliser le personnel aux mesures de cybersécurité, demeurer vigilant sur les courriels reçus, ne pas ouvrir les pièces jointes suspectes, limiter les navigations internet aux seuls rapports professionnels	-Responsabiliser le personnel. 1) En rappelant aux utilisateurs les points suivants : - mise en place de mots de passe forts sur les comptes de messagerie et de réseaux sociaux - demeurer vigilants sur les courriels reçus dont l'origine n'est pas certaine. En cas de doute, ne pas ouvrir les pièces jointes, ni suivre les liens Internet y figurant. Vérification de l'origine, analyse antivirus, ou ouverture dans un environnement dédié - minimiser les navigations vers des sites Internet n'ayant pas de rapport avec l'activité professionnelle ; - Signaler toute suspicion d'attaque,rendre compte aux responsables locaux de la sécurité des systèmes d'information de tout comportement anormal du poste de travail. 2) En invitant les responsables organiques à s'assurer auprès des hébergeurs des sites Internet à protéger d'une capacité d'intervention rapide en cas d'incident affectant l'un de ceux-ci. B) Protéger logiquement ses systèmes d'information en conduisant dans les meilleurs délais les actions suivantes : - Appliquer en priorité les mises à jour des postes utilisateur, en particulier antivirus, le système d'exploitation et le navigateur internet et les greffons (flash, java, etc). - Appliquer le filtrage des pièces jointes aux messages en fonction de leur extension. - Configurer des restrictions logicielles sur les postes de travail pour empêcher l'exécution de codes à partir d'une liste noire de répertoires. Fiches de recommandations disponibles sur le site Internet de l'ANSSI et du CERT-FR 1. guide d'hygiène : http://.ssi.gouv.fr/entreprise/guide/guide-dhygiene-informatique. 2. Guide de bonnes pratiques : http://ssi.gouv.fr/entreptrie/guide/guide-des-bonnes-pratiques-de-informatique/ Dénis de service-Prévention et réaction : www.cert.ssi.gouv.fr/site/CERTA-2012-INF-001 3. Sécurisation des sites web : http://www.ssi.gouv.fr/entreprise/guide/recommandations-pour-la-securisation-des-sites-web/ 4. Comprendre et anticiper les attaques en DDos : http://www.ssi.gouv.fr/entreprise/guide/comprendre-et-anticiper-les- attaques-ddos/ 5. Défiguration dénis de services : www.ssi.gouv.fr/uploads/2015/02/Fiche_d_information_Administrateus.pdf, 6. Cyberattaques, prévention, réaction :	CYB

		www.ssi.gouv.fr/uploads/2015/02/Fiche_des_bonnes_pratiques_en_cybersecurite.pdf 7. Conduite à tenir en cas d'intrusion : www.cert.ssi.gouv.fr/site/CERTA-22002-INF-002 8. Défiguration de sites : www.cert.ssi.gouv.fr/site/CERTA-INF-002 9. Mesures de prévention relatives à la messagerie : www.cert.ssi.gouv.fr/site/CERTA-2000-INF-002 10. Politique de restrictions logicielles sous Windows : www.ssi.gouv.fr/entreprise/guide:recommandations-pour-la-mise-en-oeuvre-dune-politique-de-restrictions-logicielles-sous-windows **Notifications d'incidents :** **www.ssi.gouv.fr/agence/contacts/cossicert-fr**	

Action	Libellé mesure	Commentaires	N° mesure
	Renforcer la surveillance et le contrôle	***Manifestations en extérieur :*** Effort particulier de vigilance à porter : -aux activités culturelles, conférences, congrés, - aux activités sportives ; - aux activités et aux déplacements de groupes de mineurs. - Ces dispositions ne font pas obstacle à la liberté de l'organisateur de renoncer à la tenue d'une manifestation dès lors qu'il le juge nécessaire, soit parce qu'il estime ne pas être en mesure de satisfaire pleinement à ces obligations de sécurité du public ou des participants, soit en fonction de circonstances liées notamment à la thématique de la manifestation. Un contact avec les services de sécurité intérieure locaux est recommandé afin d'aider les organisateurs dans leur appréciation du risque.	RSB 11-01 RSB 12-01 RSB 13-01 **RSB 20-03** **(nouvelle mesure)**
	Restreindre voire interdire le stationnement et/ou la circulation aux abords des installations et bâtiments désignés	En lien avec les préfectures, renforcement de la vigilance	BAT 11-02 BAT 12-02 BAT 13-02
	Renforcer la surveillance aux abords des installations et	La sensibilisation à la détection et au signalement de comportements suspects doit être réalisée.	BAT 11-03 BAT 12-03 **BAT 20-02** **(nouvelle mesure)**

	bâtiments désignés		
	Renforcer la surveillance interne et limiter les flux (dont interdiction de zone)	Renforcement de la surveillance interne dans : - les bâtiments officiels. En s'appuyant sur les guides de bonnes pratiques. Pour les points d'importance vitale relevant du secteur.	BAT 31-01
	Renforcer le niveau de sécurité des systèmes d'information	*www.ssi.gouv.fr:en-cas-d'incident*	CYB

Action	Libellé mesure	Commentaires	N° mesure
	Renforcer la protection contre les intrusions dans les systèmes d'information	Appliquer en priorité les mises à jour des postes utilisateur et les systèmes d'information utilisés ; Appliquer des règles de filtrage entre les réseaux (interne et externe) ; Limiter les impacts d'une attaque en déni de service, Mettre en place des sauvegardes régulières de toutes les données critiques. Élever la fréquence de sauvegarde à un niveau permettant la reprise des activités en cas d'altération des données.	CYB 42-01 CYB 42-02 CYB 43-01 CYB 43-02
	Renforcer la protection contre les attaques en déni de service		
	Contrôler les accès des personnes, des véhicules et des objets entrants (dont le courrier)	Contrôles renforcés aux accès des : Maintien et renforcement supplémentaire du contrôle des accès dans les bâtiments universitaires et de recherche, les écoles, les bâtiments officiels. Le ciblage, les modalités et l'intensité de ce contrôle sont à définir par les chefs d'établissement, les présidents d'universités, les directeurs d'organismes, en lien avec les préfectures et les autorités administratives ou académiques. Dans la mesure du possible, les contrôles doivent être au moins aléatoires sinon systématiques. Les contrôles peuvent se traduire par des inspections visuelles des sacs, des filtrages des entrées, une présence renforcée des services de sécurité. Sur l'ensemble du territoire, renforcement supplémentaire dans les lieux de culte, écoles confessionnelles, établissements culturels et symboliques sensibles des diverses confessions religieuses. Une attention particulière au contrôle des accès sera portée lors des manifestations pouvant se dérouler dans l'enceinte des établissements (journées portes ouvertes, congrés, conférences , inscriptions universitaires…). Ces manifestations doivent être signalées à la préfecture et	BAT 21-01 BAT 22-01 BAT 23-01 BAT 31-01 RSB 23-02

		au rectorat. *Les mesures de contrôle peuvent notamment consister en des dispositifs de filtrage et d'inspection visuelle des sacs.*	
	Tenir à jour les inventaires des stocks de matières dangereuses pour détecter rapidement les vols ou disparitions et signaler ces disparitions aux autorités	Signaler tous vols, disparitions ou transactions suspectes de précurseurs d'explosifs et agents NRBC au point de contact national : - pôle judiciaire de la gendarmerie nationale : pixaf@gendarmerie.interieur.gouv.fr Tél H/24 : 01.78.47.34.29. et au service spécialisé du HFDS : Etablir et mettre à jour les plans particuliers de protections (PPP), les Plans d'Opérations Internes (POI) les Plans d'Urgences Interne (PUI) les Plans de Protections Externes (PPE)relatifs au transport de marchandises dangereuses à hauts risques. Tenir à jour les	IMD 10-06 IMD 10-02
	Protéger les établissements Site SEVESO	Les directeurs des établissements 'enseignement supérieur et de recherche doivent poursuivent les efforts de sécurisation de leurs sites en s'appuyant sur le déploiement de leur plan de sécurité d'établissement (PSE), le renforcement des relations avec les préfectures et les forces de sécurité intérieure et la mise en œuvre d'actions de formations à l'intention de l'ensemble de leur personnel.	

NB : Les mesures sont numérotées avec les critères suivants :

- trigramme de domaine :

ALR : Alerte	BAT : Installations et bâtiments
CYB : CYBER	IMD : Installations et matières dangereuses
RSB : Rassemblements et zones ouvertes au public	

- numéro d'ordre (dans le tableau du plan Vigipirate) de la mesure de 01 à 0x pour les mesures du socle et de 01 à 0x pour les mesures additionnelles.

Exemple : la mesure BAT 13-04 : est une mesure du secteur installations et bâtiments (BAT), s'inscrit dans le 1er objectif du secteur (adapter la sûreté externe).