Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère Culture Communication

Paris, le 8 septembre 2016

**Note**
**de posture VIGIPIRATE**

LE HAUT FONCTIONNAIRE DE DÉFENSE ET DE SÉCURITÉ

n° 2016/06

Objet : Adaptation de la posture VIGIPIRATE « rentrée 2016 ».

La posture VIGIPIRATE « rentrée 2016 » **s'applique à partir de ce jour** et prend en considération les vulnérabilités propres à la période de rentrée scolaire, de reprise générale de l'activité et l'actualisation de l'évaluation de la menace terroriste. Elle s'applique, sauf événements particuliers, **jusqu'au 1er décembre**.

Le niveau « alerte-attentat » s'applique en Île-de-France et dans le département des Alpes-Maritimes. La « vigilance renforcée » est maintenue sur le reste du territoire national.

Cette adaptation de posture met l'accent sur :

- la vigilance renforcée autour des écoles, établissements scolaires et **établissements d'enseignement supérieur et de recherche. Concernant ces derniers, un guide des bonnes pratiques sera prochainement diffusé par le ministère chargé de l'enseignement supérieur et disponible sur le site http://www.encasdattaque.gouv.fr**

- le maintien de la vigilance dans le domaine des transports : fin des congés d'été et vacances de la Toussaint (aéroports, gares des grandes agglomérations, transports en commun, navires à passagers) ;

**- la poursuite de la sensibilisation aux bons comportements au sein des établissements de forte affluence.**

Les activités à forte affluence doivent être signalées aux préfectures concernées et les organisateurs doivent veiller à assurer une sécurité optimale en lien avec les forces de l'ordre, les autorités préfectorales restant juges du niveau de sécurité à atteindre pour autoriser ces activités.

L'ensemble des actions de vigilance, de surveillance et de contrôle est récapitulé dans le tableau ci-dessous (réf : plan VIGIPIRATE mesures publiques).

| N° mesure | Mesure | Commentaires |
|---|---|---|
| ALR 11-01 | Activer les cellules de veille et d'alerte et les cellules de crise | Les cellules de crise des ministères sont activées en tant que de besoin. |
| ALR 11-02 | Diffuser l'alerte au grand public | - affichage du logo « VIGIPIRATE Alerte-attentat » en Île-de-France et dans le département des Alpes-Maritimes et « VIGILANCE » hors Île-de-France, aux endroits où des mesures de protection renforcées sont mises en œuvre ;<br>- diffusion de messages d'appel à la vigilance dans les établissements recevant du public (ERP), y compris en langues étrangères ;<br>- information claire des visiteurs et spectateurs sur les sites web de chaque établissement concernant les mesures de contrôle en vigueur ;<br>- information claire et visible à l'entrée de l'établissement : utiliser les pictogrammes en ligne sur le site<br>http://www.culturecommunication.gouv.fr/Actions-de-renforcement-et-de-surveillance-des-lieux-culturels<br>- application smartphone SAIP d'alerte aux populations, principalement conçue pour diffuser les alertes sur des attentats |
| RSB 11-01<br>RSB 12-01<br>RSB 13-01 | Renforcer la surveillance et le contrôle | **Manifestations en extérieur**<br>***1) dans une enceinte close d'un établissement :***<br>- contrôle visuel systématique des visiteurs en demandant à ceux ayant des vêtements amples, susceptibles de dissimuler une arme automatique, de les ouvrir, ainsi que du contenu de leurs sacs ;<br>- interdiction des valises et des sacs de grande contenance.<br>Toute personne refusant le contrôle doit se voir interdire l'entrée de l'établissement.<br>***2) sur la voie publique :*** ces manifestations sont soumises à des restrictions qui peuvent être plus importantes selon les directives préfectorales.<br>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 ses obligations de sécurité du public, soit en fonction de circonstances spécifiques liées notamment à la thématique de la manifestation. Un contact avec les services de police locaux peut aider les organisateurs dans leur appréciation du risque.<br>**Un effort particulier de vigilance doit porter sur les rassemblements liés aux grands événements.** |

| | | |
|---|---|---|
| BAT 11-02<br>BAT 12-02<br>BAT 13-02 | Restreindre voire interdire le stationnement et/ou la circulation aux abords des installations et bâtiments désignés | A l'appréciation des préfets pour le ciblage.<br>**En accord avec les forces de police, des mesures de sécurité passive (barriérage, plots béton, chicane...), voire la restriction ou l'interdiction de circulation peuvent utilement être déployées.** |
| BAT 11-03<br>BAT 12-03 | Renforcer la surveillance aux abords des installations et bâtiments désignés | Renforcement de la vigilance externe par l'installation de dispositifs de vidéoprotection, prioritairement pour les ERP **et les établissements d'enseignement supérieur** |
| BAT 21-01<br>BAT 22-01<br>BAT 23-01 | Contrôler les accès des personnes, des véhicules et des objets entrants (dont le courrier) | 1) renforcement du contrôle des **visiteurs / spectateurs** :<br>- pour les établissements équipés de portiques : passage systématique sous portique ;<br>- pour les établissements équipés de magnétomètres : utilisation systématique.<br>- **valises et sacs de grande contenance** : interdits dans les ERP non équipés de scanner à rayons X.<br>Pour les établissements concernés, il convient d'informer le public (site web et affichage) de cette mesure, et de modifier le règlement intérieur de l'établissement.<br>Toute personne refusant l'un de ces contrôles doit se voir interdire l'entrée de l'établissement.<br>Toutefois, pour les chefs d'établissement de l'enseignement supérieur du secteur de la culture qui reçoivent des étudiants, ces derniers peuvent, selon la situation de leur établissement, autoriser leurs professeurs et leurs étudiants à introduire des valises, des sacs et des étuis d'instruments de musique après contrôle visuel du contenu.<br>2) pour le **personnel** : badge (ou pièce d'identité) obligatoire pour l'accès à l'établissement. A l'appréciation des chefs d'établissement et selon la situation de leur établissement, autorisation est donnée à ceux-ci de procéder au **renforcement des contrôles** (inspection visuelle des sacs) pour les personnels des manifestations extérieures, les prestataires extérieurs, les personnels intérimaires et temporaires, et en tant que de besoin selon la taille, la configuration, le site ou le caractère symbolique de l'établissement, pour les personnels permanents, après information/consultation du CHSCT spécial d'établissement consacré aux mesures de sûreté et de sécurité.<br>3) limitation des **accès aux sites** :<br>- accès visiteurs : limitation du nombre d'accès à l'initiative des chefs d'établissement ;<br>- autres accès : les accès réservés à du personnel spécifique (artistes, prestataires extérieurs, agents de l'établissement) doivent faire l'objet d'un renforcement des contrôles tel qu'indiqué ci-dessus. |

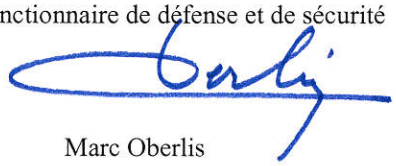
| | | |
|---|---|---|
| | | 4) **véhicules entrants** : contrôle systématique et vérification de la marchandise. |
| **BAT 31-01** | **Renforcer la surveillance interne et limiter les flux (dont interdiction de zone)** | **Limitation des flux de visiteurs si l'affluence est jugée trop importante, notamment en Ile-de-France et dans les Alpes-Maritimes** |
| CYBER | Protéger logiquement ses systèmes d'information | 1) Conseils aux utilisateurs<br>- demeurer vigilant sur les courriels reçus et, en cas de doute, ne pas ouvrir les pièces jointes ni cliquer sur les liens internet y figurant ;<br>- limiter les navigations vers des sites internet n'ayant pas de rapport avec l'activité professionnelle ;<br>- rendre compte aux responsables locaux de la sécurité des systèmes d'information de tout comportement anormal du poste de travail.<br><br>2) Conseils aux responsables organiques<br>- assurer une revue des droits des comptes les plus privilégiés et en assurer une supervision ;<br>- contrôler l'application de la politique des mots de passe et renouveler les mots de passe des comptes les plus privilégiés ;<br>- vérifier ou mettre en place les mesures de prévention en matière de déni de service.<br><br>***Vous pouvez consulter les notes d'information et les guides de l'ANSSI sur le site www.ssi.gouv.fr/administration/bonnes-pratiques/ concernant notamment :***<br>***- guide d'hygiène***<br>***- guide de bonnes pratiques***<br>***- dénis de service (prévention et réaction)***<br>***- sécurisation des sites web***<br>***- comprendre et anticiper les attaques en DDoS***<br>***- défigurations de sites***<br>***- cyberattaquess (prévention, réaction)***<br>***- conduite à tenir en cas d'intrusion***<br>***- mesures de prévention relatives à la messagerie***<br>***- politique de restrictions logicielles sous Windows*** |

**Ces consignes doivent être retransmises aux acteurs du champ culturel conformément à la chaîne d'information et d'alerte du MCC (cf note du directeur de cabinet du 23 décembre 2015), notamment, pour les DRAC, les acteurs considérés comme sensibles (cf. votre cartographie régionale), afin qu'ils organisent leur propre protection, et d'en rendre compte au préfet de chaque département.**

Trois guides de bonnes pratiques sont à votre disposition sur le site du ministère :
http://www.culturecommunication.gouv.fr/Actions-de-renforcement-et-de-surveillance-des-lieux-culturels
- guide à destination des organisateurs de rassemblements et festivals culturels
- guide à destination des dirigeants de salles de spectacle, de cinémas ou de cirques
- guide à destination des dirigeants d'établissements culturels patrimoniaux (musées, monuments historiques, archives et bibliothèques)
Ces guides ont vocation à être diffusés le plus largement possible.

Enfin, il convient de rappeler à vos collaborateurs appelés à effectuer des missions à l'étranger de consulter préalablement le site du ministère des affaires étrangères http://www.diplomatie.gouv.fr/fr/conseils-aux-voyageurs/ afin de prendre connaissance des consignes de sécurité spécifiques au pays concerné et à s'inscrire sur le site *Ariane* du ministère des affaires étrangères et du développement international.

Le Haut fonctionnaire de défense et de sécurité



Marc Oberlis