**Plan VIGIPIRATE**
**Tableau des mesures publiques**
**(posture en vigueur au 29 août 2016)**

| Numéro de mesure | Mesures | Niveau de protection | POSTURE ALERTE-ATTENTAT en IDF à compter du 14 décembre 2015 et dans les ALPES MARITIMES à compter du 14 juillet 2016<br>STATUT | ACTEURS | POSTURE pour la rentrée 2016 (activation le 29/08/2016)<br><br>COMMENTAIRES |
|---|---|---|---|---|---|
| | | | ***Légende*** | **Menant**<br>Concourant | ***Mention nouvelle par rapport à la précédente posture*** |
| ALR 11-01 | activer les cellules de veille et d'alerte et les cellules de crise | publique | active | **MININT**<br>Tous ministères | Les cellules de crise des ministères sont activées en tant que de besoin. |
| ALR 11-02 | diffuser l'alerte au grand public | publique | active | **SIG**<br>**CIC**<br>Tous ministères | L'application smartphone d'alerte aux populations "SAIV" – principalement conçue pour diffuser les alertes sur des attentats – est entrée en service en juin 2016. Il est donc demandé aux préfets d'intégrer cette nouvelle fonctionnalité dans leurs plans de communication avec les citoyens, et le cas échéant, de l'utiliser pour relayer un message local d'alerte et les consignes comportementales adaptées. |
| RSB 11-01<br>RSB 12-01<br>RSB 13-01 | renforcer la surveillance et le contrôle | publique | active<br>RSB 13-01 | **MININT**<br>**Collectivités**<br>**Opérateurs**<br>**MEN**<br>**MASS**<br>**MAAF**<br>**Collectivités** | L'effort de vigilance porte sur les rassemblements **liés aux fêtes religieuses (musulmane le 13 septembre, chrétienne le 1er novembre, juives à l'automne)** et sur les sites touristiques **(jounées européennes du patrimoine les 17 et 18 septembre).** |
| 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) | publique | active<br>BAT 23-01 | **Tous ministères**<br>**Collectivités**<br>**Opérateurs** | De manière ciblée selon l'appréciation des ministères concernés pour les sites militaires, les sites touristiques symboliques, les services de l'Etat, les ambassades des pays occidentaux, les points d'importance vitale. |
| 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) | publique | active<br>BAT 23-01 | **Tous ministères**<br>**Collectivités**<br>**Opérateurs** | **Contrôles renforcés de l'accès des personnes à l'entrée des écoles, établissements scolaires, établissements de l'enseignement supérieur et de la recherche. Effort de vigilance et de protection autour des principaux sites touristiques lors des journées européennes du patrimoine (17 et 18 septembre). Contrôles renforcés aux accès des établissements de santé, médico-sociaux et sociaux. Maintien des contrôles - non systématiques - à l'entrée des grands espaces commerciaux. Effort de contrôles systématiques aux accès des espaces de loisir.** |
| BAT 31-01 | Renforcer la surveillance interne et limiter les flux (dont interdiction de zone) | publique | active | **Tous ministères**<br>**Collectivités**<br>**Opérateurs** | De manière ciblée selon l'appréciation des ministères concernés pour les sites militaires, les sites touristiques symboliques, les services de l'Etat, les ambassades des pays occidentaux, les points d'importance vitale.<br>Renforcement de la surveillance interne aux abords des organes de presse, des grands magasins et espaces commerciaux, des lieux de culte, des sites touristiques, des écoles et établissements scolaires - en particulier les écoles confessionnelles - des bâtiments officiels en Île-de-France et dans les Alpes-Maritimes. |

**Plan VIGIPIRATE**
**Tableau des mesures publiques**
**(posture en vigueur au 29 août 2016)**

| Numéro de mesure | Mesures | Niveau de protection | POSTURE ALERTE-ATTENTAT en IDF à compter du 14 décembre 2015 et dans les ALPES MARITIMES à compter du 14 juillet 2016<br>STATUT | ACTEURS | POSTURE pour la rentrée 2016 (activation le 29/08/2016)<br><br>COMMENTAIRES |
|---|---|---|---|---|---|
| IMD 10-01 | Tenir à jour les inventaires des stocks de matières dangereuses pour détecter rapidement les vols ou disparitions et signaler ces disparitions aux autorités | publique | socle | **dont MASS** | Signaler tous vols, disparitions ou transactions suspectes d'équipements de protection ou de précurseurs d'explosifs (ou agents NRBC) au point de contact national : pôle judiciaire de la gendarmerie national – pixaf@gendarmerie.interieur.gouv.fr – Tph H/24 : 01.78.47.34.29. Références du code de la santé publique : article R5132-58 et article R5132-59. |
| IMD 10-02 | Établir et mettre à jour les plans particuliers de protection (PPP), les plans d'opération internes (POI), les plans d'urgence internes (PUI), les plans particuliers d'interventions (PPI), les plans de protection externes (PPE) et les plans de sûreté relatifs aux transports de marchandises dangereuses à haut risque | publique | socle | **MININT**<br>**Collectivités**<br>MEDDE<br>Tous ministères<br>Opérateurs | cf. instruction du Gouvernement du 30 juillet 2015 relative au renforcement de la sécurité des sites Seveso contre les actes de malveillance (NOR : DEVP1518240J). |
| IMD 13-04 | Restreindre, dérouter ou arrêter les trafics de matières dangereuses | publique | active | | Des mesures d'interdiction de transport de matières dangereuses peuvent être prises par les préfets, au cas par cas, |
| CYB | Avoir les ressources humaines permettant la cybersécurité | publique | socle | **Tous ministères**<br>**Collectivités**<br>**Opérateurs** | Responsabiliser le personnel. **Sensibiliser le personnel :**<br>**- à la mise en place de mots de passe forts sur les comptes de messagerie et de réseaux sociaux;**<br>**- contre les attaques en déni de service et les défigurations et les approvisionner en éléments de langage et de communication sur ces attaques;**<br>**Concernant les messages électroniques, inviter les utilisateurs à :**<br>**- porter une attention toute particulière à l'ouverture des messages électroniques dont l'origine n'est pas certaine ;**<br>**- ne pas suivre les liens figurant dans un message électronique. En cas de nécessité d'accès, ils privilégieront la navigation directe sur le site Internet référencé ;**<br>**- n'ouvrir les pièces jointes aux messages qu'en cas de nécessité et avec précaution (vérification de l'origine, analyse antivirus ou ouverture dans un environnement dédié) ;**<br>**- signaler toute suspicion d'attaque auprès du responsable de la sécurité des systèmes d'information.** |
| CYB | Protéger logiquement ses systèmes d'information | publique | socle | **Tous ministères**<br>**Collectivités**<br>**Opérateurs** | Protéger logiquement ses systèmes d'information<br>**- Appliquer en priorité les mises à jour des postes utilisateur, en particulier les antivirus, le système d'exploitation et le navigateur Internet et les greffons (Flash, Java, etc.) ;**<br>**- Appliquer un filtrage des pièces jointes aux messages électroniques en fonction de leur extension ;**<br>**- Configurer des restrictions logicielles sur les postes de travail pour empêcher l'exécution de codes à partir d'une liste noire de répertoires.** |

**Plan VIGIPIRATE**
**Tableau des mesures publiques**
**(posture en vigueur au 29 août 2016)**

| Numéro de mesure | Mesures | Niveau de protection | POSTURE ALERTE-ATTENTAT en IDF à compter du 14 décembre 2015 et dans les ALPES MARITIMES à compter du 14 juillet 2016<br>STATUT | ACTEURS | POSTURE pour la rentrée 2016 (activation le 29/08/2016)<br><br>COMMENTAIRES |
|---|---|---|---|---|---|
| CYB | Protéger logiquement ses systèmes d'information | publique | socle | **Tous ministères**<br>**Collectivités**<br>**Opérateurs** | Protéger logiquement ses systèmes d'information<br>**- Appliquer en priorité les mises à jour des postes utilisateur, en particulier les antivirus, le système d'exploitation et le navigateur Internet et les greffons (Flash, Java, etc.) ;**<br>**- Appliquer un filtrage des pièces jointes aux messages électroniques en fonction de leur extension ;**<br>**- Configurer des restrictions logicielles sur les postes de travail pour empêcher l'exécution de codes à partir d'une liste noire de répertoires.**<br>**Fiches de recommandations disponibles sur le site Internet de l'ANSSI et du CERT-FR:**<br>**1. Guide d'hygiène : http://www.ssi.gouv.fr/entreprise/guide/guide-dhygiene-informatique**<br>**2. Guide des bonnes pratiques : http://www.ssi.gouv.fr/entreprise/guide/guide-des-bonnes-pratiques-de-linformatique/**<br>**3. Dénis de service – Prévention et réaction : www.cert.ssi.gouv.fr/site/CERTA-2012-INF-001**<br>**4. Sécurisation des sites web : http://www.ssi.gouv.fr/entreprise/guide/recommandations-pour-la-sécurisation-des-sites-web/**<br>**5. Comprendre et anticiper les attaques en DDoS : http://www.ssi.gouv.fr/entreprise/guide/comprendre-et-anticiper-les-attaques-ddos/**<br>**6. Défigurations, dénis de services : www.ssi.gouv.fr/uploads/2015/02/Fiche_d_information_Administrateurs.pdf,**<br>**7. Cyberattaques, prévention, réaction :**<br>**www.ssi.gouv.fr/uploads/2015/02/Fiche_des_bonnes_pratiques_en_cybersecurite.pdf**<br>**8. Conduite à tenir en cas d'intrusion : www.cert.ssi.gouv.fr/site/CERTA-2002-INF-002**<br>**9. Défiguration de sites : www.cert.ssi.gouv.fr/site/CERTA-2012-INF-002**<br>**10. Mesures de prévention relatives à la messagerie : www.cert.ssi.gouv.fr/site/CERTA-2000-INF-002**<br>**11. 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**<br><br>**Notification d'incidents :**<br>**www.ssi.gouv.fr/agence/contacts/cossicert-fr** |
| AIR 22-01<br>AIR 23-01 | Appliquer un taux de palpation des passagers et de fouille des bagages de cabine supérieur à la réglementation en vigueur sur certains aérodromes désignés | publique | | **MEDDE**<br>**MININT**<br>**Opérateurs** | Mesure prête à être activée sur très court préavis, sur des vols ciblés et de manière limitée dans le temps. |
| AIR 30-02 | Faire appel aux armées pour des opérations de surveillance des zones publiques des aérogares | publique | socle | **MININT**<br>MINDEF<br>MEDDE | Ensemble des points d'application à déterminer en ciblant en priorité les grands aéroports internationaux ; à adapter en concertation préfets de zone - officiers généraux de zone de défense. |
| AIR 31-02 | Diffuser des messages d'information et des consignes particulières aux usagers | publique | active | **Opérateurs** | Procéder à des appels à la vigilance du public. |

**Plan VIGIPIRATE**
**Tableau des mesures publiques**
**(posture en vigueur au 29 août 2016)**

| Numéro de mesure | Mesures | Niveau de protection | POSTURE ALERTE-ATTENTAT en IDF à compter du 14 décembre 2015 et dans les ALPES MARITIMES à compter du 14 juillet 2016<br>STATUT | ACTEURS | POSTURE pour la rentrée 2016 (activation le 29/08/2016)<br><br>COMMENTAIRES |
|---|---|---|---|---|---|
| TER 11-02 | Diffuser des messages d'information et des consignes particulières aux usagers | publique | active | **Opérateurs** | Procéder à des appels à la vigilance du public, et inviter les usagers à signaler à l'opérateur tout incident de sûreté. Les appels à la vigilance du public, y compris en langues étrangères, pour rappeler de ne pas laisser de colis sans surveillance sont effectués régulièrement, notamment pendant les plages horaires de grande affluence. |
| TER 21-02 | Diffuser des messages d'information et des consignes particulières aux usagers | publique | active | **Opérateurs** | Procéder à des appels à la vigilance du public, et inviter les usagers à signaler à l'opérateur tout incident de sûreté. Les appels à la vigilance du public, y compris en langues étrangères, pour rappeler de ne pas laisser de colis sans surveillance sont effectués régulièrement, notamment pendant les plages horaires de grande affluence. |
| TER 31-02 | Diffuser des messages d'information et des consignes particulières aux usagers | publique | active | **Opérateurs**<br>**MININT** | Procéder à des appels à la vigilance du public, en incitant les usagers à signaler à l'opérateur tout incident de sûreté. Les appels à la vigilance du public, y compris en langues étrangères, pour rappeler de ne pas laisser de colis sans surveillance sont effectués régulièrement, notamment pendant les plages horaires de grande affluence. |