

Amiens, le 22 mars 2017



## Le Recteur

Dossier suivi par  
Jean-Michel Carron  
Directeur de Cabinet  
Mel : [ce.cabinet@ac-amiens.fr](mailto:ce.cabinet@ac-amiens.fr)  
Tel: 0322826952

Emmanuel Véziat  
Conseiller Défense du Recteur  
Mel : [emmanuel.veziat@ac-amiens.fr](mailto:emmanuel.veziat@ac-amiens.fr)  
Tel.: 0322823944

20, boulevard  
d'Alsace-Lorraine  
80063 Amiens cedex 9

## LE RECTEUR DE L'ACADÉMIE D'AMIENS

*Chancelier des universités*

à

- Messieurs les Inspecteurs d'académie, directeurs académiques des services de l'Éducation nationale de l'Aisne, de l'Oise et de la Somme
- Madame et messieurs les Directeurs diocésains
- Monsieur le Secrétaire général d'académie
- Monsieur le responsable de la sécurité des systèmes d'information DSIN / Rectorat
- Mesdames et messieurs les chefs d'établissement public et privé
- Mesdames et messieurs les IEN de circonscription
- Mesdames et messieurs les directeurs d'écoles

**Référence** : note du HFDS n°2017-371

**Objet** : adaptation des mesures VIGIPIRATE – « Printemps 2017 »

Cette nouvelle posture prend en compte les vulnérabilités propres au 2<sup>e</sup> trimestre 2017 et s'applique jusqu'au 22 juin 2017. La menace terroriste se maintient durablement à un niveau très élevé avec un état d'urgence prolongé jusqu'au 15 juillet prochain.

L'accent est notamment mis sur :

- la sécurisation des bâtiments et des lieux de rassemblements publics liés aux campagnes et aux scrutins des élections présidentielles et législatives,
- la vigilance dans les lieux de très forte fréquentation du public (édifices religieux, espaces de commerce ou de loisirs, établissements d'enseignement, rassemblements festifs, politiques, culturels ou sportifs, transports...).

La pleine efficacité des mesures arrêtées repose sur la sensibilisation des acteurs de terrain ainsi que sur l'adaptation des dispositifs de sécurité existants à la sensibilité particulière de la période couverte par cette posture.

Les écoles et établissements qui n'auraient pas encore procédé à un exercice de sécurité de type « attentat-intrusion » doivent le programmer sans délai. L'actualité récente rappelle la nécessité de ce type de sensibilisation et de préparation.

En application du nouveau plan Vigipirate entré en vigueur le 1<sup>er</sup> décembre 2016, l'ensemble du territoire national est maintenu au niveau « sécurité renforcée risque attentat ». A ce titre, les anciens logos « alerte attentat » doivent être enlevés et remplacés par les logos « sécurité renforcée risque attentat » à l'entrée des établissements scolaires : <http://www.gouvernement.fr/risques/le-citoyen-au-coeur-du-nouveau-dispositif-vigipirate>

Pour les voyages et sorties scolaires, nous vous rappelons :

- la nécessité impérieuse d'informer les autorités académiques des différents déplacements que vous organisez,
- la nécessité de faire preuve d'une vigilance renforcée, que ce soit sur le territoire national comme à l'étranger, en vous conformant strictement aux prescriptions des forces de l'ordre et des différents opérateurs,
- la proscription de tout quartier libre, la surveillance des élèves devant être permanente et continue.
- la nécessité, pour les déplacements à l'étranger, de vous conformer aux consignes du ministère des Affaires étrangères et de vous inscrire sur le site Ariane : <https://pastel.diplomatie.gouv.fr/fildariane/dyn/public/login.html>

Mon cabinet et moi-même restons à votre disposition pour tout renseignement complémentaire sur cette nouvelle posture.

Je sais pouvoir compter sur la plus grande attention avec laquelle vous mettrez en œuvre ces mesures et vous en remercie vivement.



Valérie CABUIL

## Calendrier / contexte général

### Mars

DATES	LIEU	EVENEMENTS
22 mars au 25 juin	Lille	Lille 3000
24 au 27 mars	Paris	37 <sup>e</sup> édition du Salon du Livre 2017
25 mars : Annonciation (fête chrétienne)		
16 au 19 mars	Paris	Salon mondial du tourisme

3/6

### Avril

DATES	LIEU	EVENEMENTS
1 <sup>er</sup> avril au 2 mai	France	Vacances de printemps (Environ 4 millions de nuitées dans les stations de ski toutes zones confondues)
9 avril : Les Rameaux (fête chrétienne)		
9 avril	Paris	41 <sup>e</sup> Marathon de Paris (60 000 personnes attendues)
11 au 18 avril : Pessa'h (fête juive)		
13 au 16 avril : semaine sainte (Vigile pascale le 15 soir)		
Du 18 au 23 avril	Bourges	41 <sup>e</sup> édition du Printemps de Bourges
<i>23 avril</i>	France	1 <sup>er</sup> tour élection présidentielle
27 avril au 8 mai	Paris	Foire de Paris

### Mai

DATES	LIEU	EVENEMENTS
25 mai : Ascension (fête chrétienne)		
3 au 8 mai	Paris	Biennale internationale des métiers d'art et création au Grand Palais
5 au 21 mai	France (Paris) Allemagne (Cologne)	Championnat du monde de hockey sur glace
7 mai	France	2 <sup>e</sup> tour élection présidentielle
17 au 28 mai	Cannes	Festival de Cannes
21 mai	France	Nuit des musées
22 mai au 11 juin	Paris	Roland-Garros
24 au 28 mai	Lyon	Les nuits sonores
25 mai au 4 juin	Bordeaux	Fête du fleuve / départ de la solitaire du Figaro
27 mai au 11 juin	Normandie (Baie du Cotentin, Caen, Omaha Beach, Ouistreham, Bessin Seulles et Mer)	D-Day Festival Normandy
27 mai au 25 juin : Ramadan (jeûne musulman)		
31 mai au 5 juin	Nîmes	Feria

**Juin**

DATES	LIEU	EVENEMENTS
4 juin : Pentecôte (fête chrétienne)		
11 juin	France	1 <sup>er</sup> tour élections législatives
11 juin au 31 juillet	Paris	Paris Jazz Festival
13 au 17 juin	Anncy	Festival international du film d'animation
15 au 22 juin	France	Baccalauréat général
16 au 20 juin	Paris	Eurosatory
17 au 18 juin	Le Mans	24h du Mans
18 juin	France	2e tour élections législatives
19 au 25 juin	Le Bourget	Salon international de l'aéronautique et de l'espace

21 juin	France	Fête de la musique
21 juin au 1 <sup>er</sup> août	France	Soldes
24 au 26 juin	Saint-Cloud	Solidays
25 juin : Aïd al-fitr (fête musulmane)		

**Juillet**

DATES	LIEU	EVENEMENTS
Juillet - août	Paris	Paris plage
1 <sup>er</sup> au 23 juillet	France	Tour de France, départ de Düsseldorf
2 juillet	Paris	Triathlon
Date non confirmée	Paris	La Marche des Fiertés



## Mesures actives VIGIPIRATE – mars 2017

5/6

Mesures	Commentaires
Diffuser l'alerte au grand public	Les anciens logos « alerte attentat » doivent être enlevés et remplacés par les logos « <b>sécurité renforcée-risque attentat</b> » à l'entrée des établissements accueillant du public
Les voyages et les déplacements	<p>Les voyages et les sorties scolaires, sont laissées à l'appréciation des autorités académiques ou des préfets compétents au regard des lieux de destination et des conditions de transport qui peuvent décider de l'annulation ou du report du déplacement.</p> <p>Les déplacements et sorties scolaires restent soumis aux règles d'organisation fixées dans les circulaires DGESCO du 21 septembre 1999 pour le premier degré et du 3 août 2011 pour le second degré.</p> <p>Pour les déplacements et voyages à l'étranger se signaler sur le site du MAE (fil d'Ariane)</p>
Contrôler les accès des personnes, des véhicules et des objets entrants (dont le courrier)	<p>Maintien et renforcement supplémentaire du contrôle des accès dans les bâtiments universitaires et de recherche, les écoles, les bâtiments officiels.</p> <p>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 préfetures et les autorités administratives ou académiques.</p> <p>Dans la mesure du possible, les contrôles doivent être au moins aléatoires sinon systématiques.</p> <p>Les contrôles peuvent se traduire par des inspections visuelles des sacs, des filtrages des entrées, une présence renforcée des services de sécurité.</p> <p>Sur l'ensemble du territoire, renforcement supplémentaire dans les lieux de culte, écoles confessionnelles, établissements culturels et symboliques sensibles des diverses confessions religieuses.</p> <p>Une attention particulière au contrôle des accès sera portée lors des manifestations pouvant se dérouler dans l'enceinte des établissements (journées portes ouvertes, journée du patrimoine, inscriptions universitaires...).</p> <p>Ces manifestations doivent être signalées à la préfeture et au rectorat.</p>
Renforcer la surveillance interne et limiter les flux.	<p>Renforcement de la surveillance interne dans les écoles - en particulier les écoles confessionnelles - les bâtiments officiels. Le ciblage, les modalités et l'intensité de ce contrôle sont à définir par le chef d'établissement en lien avec les préfetures et le rectorat pour les établissements scolaires.</p> <p>Cette mesure peut se traduire par le recours à la vidéosurveillance, des rondes de sécurité plus fréquentes...</p> <p>Un effort de vigilance porte sur les rassemblements liés aux manifestations religieuses, politiques, sportives et culturelles.</p>
Avoir les ressources humaines permettant la cybersécurité	<p>A) Responsabiliser le personnel.</p> <p>1) En rappelant aux utilisateurs les points suivants :</p> <ul style="list-style-type: none"> <li>- mise en place de mots de passe forts sur les comptes de messagerie et de réseaux sociaux</li> <li>- 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</li> <li>- minimiser les navigations vers des sites Internet n'ayant pas de rapport avec l'activité professionnelle ;</li> <li>- 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.</li> </ul> <p>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.</p>
Protéger logiquement ses systèmes d'information	<p>B) Protéger logiquement ses systèmes d'information en conduisant dans les meilleurs délais les actions suivantes :</p> <ul style="list-style-type: none"> <li>- 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).</li> <li>- Appliquer le filtrage des pièces jointes aux messages en fonction de leur</li> </ul>

	<p>extension.</p> <ul style="list-style-type: none"> <li>- Configurer des restrictions logicielles sur les postes de travail pour empêcher l'exécution de codes à partir d'une liste noire de répertoires.</li> </ul> <p>Fiches de recommandations disponibles sur le site Internet de l'ANSSI et du CERT-FR</p> <ol style="list-style-type: none"> <li>1. guide d'hygiène : <a href="http://ssi.gouv.fr/entreprise/guide/guide-dhygiene-informatique">http://ssi.gouv.fr/entreprise/guide/guide-dhygiene-informatique</a>.</li> <li>2. Guide de bonnes pratiques : <a href="http://ssi.gouv.fr/entreprise/guide/guide-des-bonnes-pratiques-de-informatique/">http://ssi.gouv.fr/entreprise/guide/guide-des-bonnes-pratiques-de-informatique/</a></li> <li>3. Dénis de service-Prévention et réaction : <a href="http://www.cert.ssi.gouv.fr/site/CERTA-2012-INF-001">www.cert.ssi.gouv.fr/site/CERTA-2012-INF-001</a></li> <li>4. Sécurisation des sites web : <a href="http://www.ssi.gouv.fr/entreprise/guide/recommandations-pour-la-securisation-des-sites-web/">http://www.ssi.gouv.fr/entreprise/guide/recommandations-pour-la-securisation-des-sites-web/</a></li> <li>5. Comprendre et anticiper les attaques en DDos : <a href="http://www.ssi.gouv.fr/entreprise/guide/comprendre-et-anticiper-les-attaques-ddos/">http://www.ssi.gouv.fr/entreprise/guide/comprendre-et-anticiper-les-attaques-ddos/</a></li> <li>6. Défiguration dénis de services : <a href="http://www.ssi.gouv.fr/uploads/2015/02/Fiche_d_information_Administrateurs.pdf">www.ssi.gouv.fr/uploads/2015/02/Fiche_d_information_Administrateurs.pdf</a>,</li> <li>7. Cyberattaques, prévention, réaction : <a href="http://www.ssi.gouv.fr/uploads/2015/02/Fiche_des_bonnes_pratiques_en_cybersecurite.pdf">www.ssi.gouv.fr/uploads/2015/02/Fiche_des_bonnes_pratiques_en_cybersecurite.pdf</a></li> <li>8. Conduite à tenir en cas d'intrusion : <a href="http://www.cert.ssi.gouv.fr/site/CERTA-22002-INF-002">www.cert.ssi.gouv.fr/site/CERTA-22002-INF-002</a></li> <li>9. Défiguration de sites : <a href="http://www.cert.ssi.gouv.fr/site/CERTA-INF-002">www.cert.ssi.gouv.fr/site/CERTA-INF-002</a></li> <li>10. Mesures de prévention relatives à la messagerie : <a href="http://www.cert.ssi.gouv.fr/site/CERTA-2000-INF-002">www.cert.ssi.gouv.fr/site/CERTA-2000-INF-002</a></li> <li>11. Politique de restrictions logicielles sous Windows : <a href="http://www.ssi.gouv.fr/entreprise/guide/recommandations-pour-la-mise-en-oeuvre-dune-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</a></li> </ol> <p>Notifications d'incidents : <a href="http://www.ssi.gouv.fr/agence/contacts/cossicert-fr">www.ssi.gouv.fr/agence/contacts/cossicert-fr</a></p>
--	--