**Annexe 1**

**Mesures publiques –Eté 2017**

|  |  |
| --- | --- |
| **Mesures** | **Commentaires** |
| activer les cellules de veille et d'alerte et les cellules de crise | Activation des cellules de veille et de crise laissée à l'appréciation des autorités académiques ou des établissements d’enseignement supérieur et de recherche. |
| ALR 11-02ALR 11-04 | Les anciens logos « alerte attentat »doivent être enlevés et remplacés par les logos **« sécurité renforcée-risque attentat** » à l’entrée des établissements accueillant du publicL’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, - Recommander le téléchargement de l'application pour Smartphone "Système d'alerte et d'information des populations" (SAIP) : <http://www.gouvernement.fr/appli-alerte-saip> |
| Les voyages et les déplacements | 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.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.Pour les déplacements et voyages à l’étranger se signaler sur le site du MAE (fil d’Ariane)<http://www.diplomatie.gouv.fr/fr/conseils-aux-voyageurs>.<https://pastel.diplomatie.gouv.fr/fildariane/dyn/public/login.html> |
| Contrôler les accès des personnes, des véhicules et des objets entrants (dont le courrier)BAT 21-0122-0123-01 |  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, congrès, conférences, inscriptions universitaires…).Ces manifestations doivent être signalées à la préfecture et au rectorat. |
| Renforcer la surveillance interne et limiter les flux.BAT 31-01Etablir et mettre à jour les plans particuliers de protections (PPP) les plans d’opérations internes (POI), les plans d’urgences internes (PUI) les plans de protections externes (PPE) relatifs aux transports de marchandises dangereuses à hauts risques.IMD10-02Tenir à jour les inventaires de stocks de matières dangereuses pour détecter rapidement les vols ou disparitions et les signaler aux autoritésIMD 10-01 | Renforcement de la surveillance interne dans les écoles qui changent d’affectation, activités sportives, culturelles, associativesLe ciblage, les modalités et l’intensité de ce contrôle sont à définir par le chef d’établissement ou le responsable des activités en lien avec les préfectures et le rectorat et les collectivités territoriales pour les établissements scolaires.Cette mesure peut se traduire par le recours à la vidéosurveillance, des rondes de sécurité plus fréquentes...Un effort de vigilance porte sur les rassemblements liés aux manifestations, sportives ,culturelles et universitaires.Une attention particulière sur les OIV, Site SevesoDe manière ciblée selon l’appréciation des autorités locales les sites, les services de l’Etat, les points d’importances vitales.Etablissements détenant des matières dangereuses, signaler tous les vols,disparitions ou transactions suspectes de précurseurs d’explosifs (ou 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 : 110 rue de grenelle 75007 ParisRestreindre le transport et le flux de trafics de matières dangereuses. |
| Avoir les ressources humaines permettant la cybersécurité  | A) 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. |
| *Protéger logiquement ses systèmes d'information* | 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-FR1. 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/>
3. Dénis de service-Prévention et réaction : [www.cert.ssi.gouv.fr/site/CERTA-2012-INF-001](http://www.cert.ssi.gouv.fr/site/CERTA-2012-INF-001)
4. Sécurisation des sites web : <http://www.ssi.gouv.fr/entreprise/guide/recommandations-pour-la-securisation-des-sites-web/>
5. Comprendre et anticiper les attaques en DDos : [http://www.ssi.gouv.fr/entreprise/guide/comprendre-et-anticiper-les- attaques-ddos/](http://www.ssi.gouv.fr/entreprise/guide/comprendre-et-anticiper-les-%20attaques-ddos/)
6. Défiguration dénis de services : [www.ssi.gouv.fr/uploads/2015/02/Fiche\_d\_information\_Administrateus.pdf](http://www.ssi.gouv.fr/uploads/2015/02/Fiche_d_information_Administrateus.pdf),
7. Cyberattaques, prévention, réaction : [www.ssi.gouv.fr/uploads/2015/02/Fiche\_des\_bonnes\_pratiques\_en\_cybersecurite.pdf](http://www.ssi.gouv.fr/uploads/2015/02/Fiche_des_bonnes_pratiques_en_cybersecurite.pdf)
8. Conduite à tenir en cas d’intrusion : [www.cert.ssi.gouv.fr/site/CERTA-22002-INF-002](http://www.cert.ssi.gouv.fr/site/CERTA-22002-INF-002)
9. Défiguration de sites : [www.cert.ssi.gouv.fr/site/CERTA-INF-002](http://www.cert.ssi.gouv.fr/site/CERTA-INF-002)
10. Mesures de prévention relatives à la messagerie : [www.cert.ssi.gouv.fr/site/CERTA-2000-INF-002](http://www.cert.ssi.gouv.fr/site/CERTA-2000-INF-002)
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](http://www.ssi.gouv.fr/entreprise/guide%3Arecommandations-pour-la-mise-en-oeuvre-dune-politique-de-restrictions-logicielles-sous-windows)

**Notifications d’incidents :****www.ssi.gouv.fr/agence/contacts/cossicert-fr** |