Annexe 6

Mesures de vigilance devant être prioritairement appliquées au sein des ministères sociaux / Posture Hiver Printemps 2026

	Numéro de mesure	Type de mesure	Intitulé de la mesure	Commentaire
	Alerte & Mobilisation			
	ALR 10-01	Socle	Disposer d'une chaîne d'alerte et d'information le plus large possible, la vérifier et la tester régulièrement.	Veiller à mettre à jour régulièrement les bases de contacts et organigrammes. Tester régulièrement la diffusion d'une alerte, y compris de manière planifiée.
	ALR 10-04	Socle	Signaler tout vol ou disparition de matières et tout indice d'événement NRBC-E.	Une vigilance particulière doit porter sur le signalement de toute transaction, vol ou disparition de matière NRBC-E (précurseurs d'explosifs, acide sulfurique, bouteilles de gaz, sources radioactives, etc.). Une fiche de recommandations pratiques, dédiée aux précurseurs d'explosifs est disponible sur le site Internet du SGDSN (https://www.sgdsn.gouv.fr/files/files/Publications/fiche-produits-chimiques-signalement-de-tout-vol-ou-utilisation-suspecte.pdf) et rappelle le point de contact national à joindre pour signaler tout événement suspect (PIXAF : 01 78 47 34 29)
	ALR 11-02	Additionnelle	Diffuser l'alerte au grand public.	Les opérateurs publics et privés doivent maintenir en place les logos « URGENCE ATTENTAT » dans les sites accueillant du public. Ces logos peuvent être téléchargés sur le site du SGDSN : https://www.sgdsn.gouv.fr/files/files/Vigipirate/logogrammes-vigipirate.pdf

	ALR 11-04	Additionnelle	Rappeler les conduites à tenir en cas d'attaque (fusillade, attaque NRBC, colis abandonné, alerte à la bombe).	Des fiches de recommandations et de bonnes pratiques sont disponibles sur le site du SGDSN : http://www.sgdsn.gouv.fr/vigipirate/le-plan-vigipirate-faire-face-ensemble ;
	ALR 11-05	Additionnelle	Interdire l'usage et/ou le transport des drones dans le périmètre déterminé	La définition des périmètres est réalisée sur la base d'arrêtés municipaux et/ou préfectoraux et procède d'une analyse locale de la menace et des vulnérabilités. Activation maintenue du fait de l'importante activité de survol de drones observée en septembre/octobre 2025.
	ALR 20-01	Socle	Élaborer et mettre à jour un plan de continuité d'activité (PCA).	Il convient d'actualiser régulièrement ces plans de continuité d'activité, les annuaires de crise, de sensibiliser les agents aux procédures d'alerte et d'organiser des exercices simples, suivis de RETEX et de plans correctifs induits.
Rassemblement & Zones ouvertes au public				
	RSB 12-05	Additionnelle	Mettre en œuvre des dispositifs de protection pour faire face aux différents modes opératoires terroristes (fusillade, explosif, chimique, véhicule bélier).	Au regard de la menace associée aux attaques par véhicules-béliers, les opérateurs sont encouragés à renforcer les dispositifs de protection passive (plots, barrières, blocs en béton, etc.) sur les accès les plus fréquentés. Ils pourront s'appuyer sur le guide réalisé par le ministère de l'intérieur : « Guide des bonnes pratiques opérationnelles de sécurisation d'un événement sur la voie publique ». Ce guide est téléchargeable : https://www.interieur.gouv.fr/Publications/Securite-interieure/Securisation-des-evenements-de-voie-publique ;

	RSB 20-03	Socle	Réglementer l'accès et la circulation des personnes dans le périmètre de protection fixé par un arrêté préfectoral.	Cette mesure s'applique sur le fondement de l'article L.226-1 du code de la sécurité intérieure. La communication ne doit pas faire connaître le détail, le ciblage, les moyens engagés dans la mise en œuvre de cette mesure. La décision du Conseil constitutionnel, du 29 mars 2018, précise : - qu'il appartient aux autorités publiques de s'assurer que soit continûment garantie l'effectivité du contrôle exercé par les officiers de police judiciaire sur les personnes privées qui sont associées à la surveillance générale de la voie publique ; - que la mise en œuvre des opérations de contrôle de l'accès et de la circulation, des palpations de sécurité, d'inspection et de fouille de bagages ainsi que de visites de véhicules soit faite sans aucune discrimination entre les personnes ; - que le renouvellement d'un périmètre de protection ne peut être décidé par le préfet qu'à la condition que celui-ci établisse la persistance du risque.
Installations & Bâtiments				
	BAT 10-01	Socle	Réglementer le stationnement et/ou la circulation aux abords des installations et bâtiments.	
	BAT 10-02	Socle	Surveiller les abords des installations et bâtiments.	Des échanges permanents doivent se tenir entre les responsables de sites et les forces de sécurité intérieure.
	BAT 10-03	Socle	Contrôler les abords des installations et bâtiments.	
	BAT 11-01 BAT 12-01 BAT 13-01	Additionnelle	Restreindre voire interdire les activités aux abords des	BAT 12-01 [DR- BAT12-01[DR-A] / à l'appréciation des préfets pour le ciblage des (…) des locaux relevant du ministère de la justice, du ministère de la Santé, des Familles, de l'Autonomie et des Personnes handicapées, (…)

			installations et bâtiments désignés.	
	BAT 11-02 BAT 12-02 BAT 13-02	Additionnelle	Restreindre voire interdire le stationnement et/ou la circulation aux abords des installations et bâtiments désignés.	BAT 12-02 : À l'appréciation des préfets pour le ciblage des établissements de santé, médicaux-sociaux et sociaux
	BAT 11-03 BAT 12-03	Additionnelle	Renforcer la surveillance aux abords des installations et bâtiments désignés.	BAT 12-03 : Vigilance particulière sur les établissements de santé de première ligne. Il est demandé aux ARS de vérifier que la liste de ces établissements a bien été transmise à leur correspondants traditionnels (Préfectures et FSI notamment)
	BAT 12-05	Additionnelle	Mettre en œuvre des dispositifs de protection pour faire face aux différents modes opératoires terroristes (fusillade, explosif, chimique, véhicule bélier).	Se référer aux fiches de recommandations et de bonnes pratiques diffusées par le SGDSN : http://www.sgdsn.gouv.fr/plan-vigipirate/les-fiches-de-recommandations-et-de-bonnes-pratiques/ ou au guide réalisé par le ministère de l'intérieur : "Guide des bonnes pratiques opérationnelles de sécurisation d'un événement de voie publique", téléchargeable sur le site INTRANET du ministère de l'Intérieur et en accès libre sur la page d'accueil Internet du Ministère : https://www.interieur.gouv.fr/Publications/Securite-interieure/Securisation-des-evenements-de-voie-publique .
	BAT 20-01	Socle	Surveiller les accès des personnes, des véhicules et des objets entrants (dont le courrier).	
	BAT 21-01 BAT 22-01 BAT 23-01	Additionnelle	Contrôler les accès des personnes, des véhicules et des	BAT 21-01 : Maintien du contrôle de l'accès aux personnes des établissements de santé, médico-sociaux et sociaux.

			objets entrants (dont le courrier).	
	BAT 30-01	Socle	Identifier les zones internes en fonction de leur sensibilité et en réglementer l'accès.	La sûreté est définie en fonction de l'évaluation des risques et des menaces auxquels est soumis l'établissement.
	BAT 30-02	Socle	Surveiller la circulation interne des bâtiments et installations.	
	BAT 31-01	Additionnelle	Renforcer la surveillance interne et limiter les flux (dont interdiction de zone).	Privilégier dans toute la mesure du possible la surveillance dynamique des espaces, la détection des comportements anormaux (ex : port de badge apparent, contrôles par sondage) et le recours à la vidéosurveillance.
	BAT 32-02	Additionnelle	Mettre en œuvre des dispositifs de protection pour faire face aux différents modes opératoires terroristes (fusillade, explosif, chimique, véhicule bélier)	Les préfets encourageront les collectivités territoriales et opérateurs privés à renforcer les dispositifs de protection passive (plots, barrières, blocs en béton) sur les lieux les plus fréquentés Tous pourront s'appuyer sur : - la fiche de recommandations Vigipirate "se protéger contre les attaques au véhicule bélier" accessible sur le site du SGDSN https://www.sgdsn.gouv.fr/files/files/Publications/fiche-se-proteger-contre-les-attaques-au-vehicule-belier.pdf ; - le guide réalisé par le ministère de l'intérieur : "Guide des bonnes pratiques opérationnelles de sécurisation d'un événement de voie publique », téléchargeable sur le site INTRANET du ministère de l'Intérieur et en accès libre sur la page d'accueil Internet du Ministère : https://www.interieur.gouv.fr/Publications/Securite-interieure/Securisation-des-evenements-de-voie-publique .
Installations & Matières dangereuses				

	IMD 10-01 IMD 10-06	Socle	Tenir à jour les inventaires des stocks de matières dangereuses pour détecter rapidement les vols ou disparitions et signaler ces disparitions aux autorités. Signaler toute transaction suspecte, vol ou disparition de matières et tout indice d'évènement NRBC-E	Signaler tous vols, disparitions ou transactions suspectes de précurseurs d'explosifs (articles L. 2351-1 et R. 2351-1 et suivants du code de la défense) et/ou d'agents chimiques dangereux (articles R. 5132-58 et 59 du code de la santé publique) au point de contact national : pôle judiciaire de la gendarmerie nationale – 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.et au service spécialisé du HFDS (hfds@sg.social.gouv.fr).
	IMD 10-02	Socle	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	S'appuyer sur la documentation communiquée par le SGDSN (exemple du PPP) : https://www.sgdsn.gouv.fr/publications/la-securite-des-activites-dimportance-vitale

			transports de marchandises dangereuses à haut risque.	
	IMD 10-03	Socle	Organiser régulièrement des exercices de test des dispositifs et de vérification de la disponibilité effective des moyens d'intervention.	
	IMD 10-07	Socle	Protéger les points névralgiques des sites désignés des véhicules béliers.	Le « guide des bonnes pratiques opérationnelles de sécurisation d'un événement de voie publique » publié par le ministère de l'Intérieur peut servir d'appui. Il est téléchargeable, en accès libre, au lien suivant https://www.interieur.gouv.fr/Publications/Securite-interieure/Securisation-des-evenements-de-voie-publique
Sécurité du numérique				
	NUM 11-01	Additionnelle	Déterminer l'ensemble des composants du SI contenant un logiciel/matériel particulier	Le cycle de vie des équipements et applicatifs informatiques conduit à l'émergence de vulnérabilités susceptibles de conduire à la compromission des systèmes d'information. Par ailleurs, certains éditeurs de solutions informatiques arrêtent la maintenance de technologies moins récentes, laissant ces technologies sans mise à jour disponible pour corriger d'éventuelles vulnérabilités. Il est donc nécessaire de cartographier régulièrement son SI et les technologies le composant afin de pouvoir agir en cas de vulnérabilité et de fin de support d'une solution informatique. Cette cartographie doit permettre d'identifier les composants du SI directement sous contrôle et ceux sous-traités. Ces travaux sont également susceptibles de supporter les travaux de construction de politiques de cybersécurité, de mettre en place une approche basée sur les risques ou de traiter plis efficacement les incidents de sécurité. L'ANSSI propose un guide permettant de mettre en place un processus de cartographie des SI

				https://cyber.gouv.fr/publications/cartographie-du-systeme-dinformation .
	NUM 11-02	Additionnelle	Rechercher sur le SI des marqueurs particuliers correspondant à une attaque	Compte tenu des campagnes d'exploitation des vulnérabilités sur les services numériques, il est recommandé de prendre connaissance des marqueurs de compromissions publiés par l'ANSSI via les rapports de la menace (https://www.cert.ssi.gouv.fr/cti/) ou au travers du feed MISP public mis à disposition par l'ANSSI (https://misp.cert.ssi.gouv.fr/feed-misp). Ces marqueurs peuvent être complétés par d'autres sources de marqueurs provenant de partenaires de confiance. Dans la mesure du possible, il convient d'ajouter ces marqueurs aux systèmes de détection disponibles (antivirus, EDR, NIDS, HIDS, etc.). Par ailleurs, il est recommandé de chercher la présence de ces marqueurs sur l'historiques des journaux disponibles afin d'identifier d'éventuelles tentatives de compromission.
	NUM 21-01	Additionnelle	Créer des alertes de sécurité en analysant les journaux ou en activant des paramètres de supervision	Afin de détecter rapidement toute activité anormale ou suspecte au sein du système d'information, il est recommandé de mettre en place des alertes de sécurité reposant sur l'analyse régulière des journaux et l'activation de paramètres de supervision adaptés. Cette démarche permet d'identifier précocement les tentatives d'intrusion, les accès non autorisés ou tout comportement inhabituel pouvant indiquer une compromission. La supervision continue des différentes composantes du système d'information, telles que les passerelles, serveurs et applications, offre la possibilité d'agir sans délai en cas de menace, de limiter la propagation d'une attaque et de faciliter la mise en œuvre de mesures correctives appropriées. La mise en place de ces dispositifs s'inscrit dans une logique d'amélioration continue de la sécurité opérationnelle.
	NUM 21-02	Additionnelle	Consulter régulièrement les sources d'information relatives aux vulnérabilités et attaques (site Internet du CERT-FR)	Afin de se prémunir d'éventuelles attaques suite à la découverte de vulnérabilités, il convient de mettre en place un processus de veille concernant la publication de ces vulnérabilités relatives aux éléments du SI opéré. Accessible notamment aux liens suivants : https://www.cert.ssi.gouv.fr/ https://www.cyberveille-sante.gouv.fr/

	NUM 31-03	Additionnelle	Absorber le trafic illégitime au niveau du réseau.	Compte tenu des attaques menées par DDoS, il est important de s'assurer que les opérateurs de services numériques, d'une part disposent d'infrastructures et composants de sécurité permettant d'absorber le trafic et qu'ils puissent transmettre à leurs clients une liste d'adresses IP illégitimes à bloquer et d'autre part, qu'ils assurent le renforcement de leurs systèmes d'information et des sites web hébergés. L'ANSSI a publié une fiche pratique sur la mise en place d'un service de protection anti-DDoS, disponible sur son site web : https://messervices.cyber.gouv.fr/documents-guides/anssi_essentiels_denis-de-service-distribues_v2.0.pdf Sur la base des informations transmises par l'ANSSI, il est nécessaire d'identifier les moyens de filtrage les plus efficaces (par exemple avec un équipement en entrée de réseau ou avec l'appui d'un opérateur de communication électronique ou un fournisseur de solution spécialisée). Il est recommandé de prendre en compte les différentes typologies d'attaques par déni de service (au niveau applicatif, spécifique à protocole ou basé sur la volumétrie) et la couverture offerte par les moyens de filtrage. Les organisations doivent ensuite mettre en place ces mécanismes de protection anti déni de service sur les infrastructures qu'ils hébergent ou demander la mise en place auprès des prestataires d'hébergement ou de communication, le cas échéant.
	NUM 31-06	Additionnelle	Sensibiliser les utilisateurs sur un risque de sécurité et un comportement à adopter.	Sensibiliser régulièrement les utilisateurs aux risques numériques et à l'application de la politique de sécurité des systèmes d'information, en particulier vis-à-vis de l'utilisation de supports amovibles, de navigation internet et d'échanges de courriels. L'attention à la sensibilité de l'information et à sa protection est également à intégrer au sein de cette sensibilisation. La non séparation des usages et matériaux personnels et professionnels, les échanges professionnels dans des lieux publics, la présence de matériaux protégés ou classifiés sur des systèmes inadéquats sont à proscrire. En complément, les utilisateurs privilégiés doivent être particulièrement sensibilisés aux bonnes pratiques afin de réduire le risque cyber. Les différents guides de l'ANSSI émettent de nombreuses recommandations en ce sens. https://cyber.gouv.fr/publications?field_type_de_publication_target_id%5B934%5D=934 https://secnumacademie.gouv.fr/
	NUM 41-01	Additionnelle	Valider et appliquer un correctif de sécurité.	Face aux vulnérabilités critiques et à l'état de la menace, il est impératif d'appliquer, dans les plus brefs délais, les correctifs de sécurité mentionnés dans les bulletins d'alerte de sécurité du CERT-FR. Les correctifs référencés dans les alertes doivent, si cela est

				nécessaire et pour des raisons d'urgence et de criticité, être appliqués en dehors des processus de maintien en condition de sécurité des systèmes d'information. De même, les correctifs mentionnés dans les avis de sécurité et qui correspondent à la veille sur plus d'une centaine de produits, doivent également être appliqués dans le cycle habituel de maintien en condition de sécurité des systèmes d'information. L'exploitation de certaines des vulnérabilités référencées permet l'accès à des comptes privilégiés pour l'attaquant et étend ses capacités de latéralisation sur les systèmes. La bonne application des correctifs de sécurité référencés doit être régulièrement contrôlée et validée. Les bulletins d'alerte de sécurité et les avis de sécurité sont disponibles sur le site https://ww.cert.ssi.gouv.fr. Les correctifs de sécurité et alertes du CERT-FR mentionnés ci-dessous doivent impérativement être appliqués pour corriger des vulnérabilités récentes particulièrement critiques : - Vulnérabilités sur les équipements de sécurité en bordure des réseaux (alertes CERTFR-2025-ALE-002, CERTFR-2025-ALE-001, CERTFR-2024-ALE-014, CERTFR-2024-ALE-013, CERTFR-2024-ALE-011, CERTFR-2024-ALE-008, CERTFR-2024-ALE-007, CERTFR-2024-ALE-006, CERTFR-2024-ALE-004, CERTFR-2024-ALE-001, CERTFR-2023-ALE-012, CERTFR-2023-ALE-008, CERTFR-2023-ALE-004, CERTFR-2022-ALE-013 du CERT-FR) De nombreux équipements comme les pares-feux et les passerelles VPN sont régulièrement la cible des attaquants qui continuent de trouver des vulnérabilités leur permettant de les compromettre pour prendre pied dans le SI ou d'obtenir des secrets d'authentification pour usurper l'identité des utilisateurs. Les vulnérabilités sur les produits de l'éditeur Ivanti (CERT-2024-ALE-001) ont ainsi été et continuent d'être activement exploitées par un acteur de la menace réputé chinois. Plus récemment encore, les solutions Palo Alto Networks GlobalProtect (CERTFR-2024-ALE-006) ou encore FortiOS (CERTFR-2024-ALE-004) ont eux aussi fait l'objet d'exploitations ciblées puis massives. Pour certains produits, les vulnérabilités remontent à 2018 et continuent d'être exploitées. Les utilisateurs doivent impérativement mettre à jour ou faire mettre à jour ces équipements et procéder au renouvellement régulier des secrets d'identification (procédure extrêmement lourde) ou basculer sur des solutions d'authentification à multiples facteurs.

				Ces exemples démontrent l'importance d'une bonne connaissance de ses systèmes d'information et de la présence d'un processus de veille et de gestion des vulnérabilités pour mieux les anticiper ou réagir rapidement. Cela est d'autant plus important qu'il peut être délicat de mettre à jour des équipements et installer des correctifs, des incompatibilités pouvant parfois émerger et rendre indisponibles des services. - Vulnérabilités sur les systèmes industriels (CVE-2023-39979 (MOXA), CVE-2023-29130 (Siemens), CVE-2023-29411 et CVE-2023-29411 (CVE-2023-29412) Certains équipements, comme des automates programmables, sont exposés sur Internet sans aucune mesure de sécurité. Une cartographie partielle de ces équipements en France a été effectuée par l'ANSSI en 2024. Elle a montré que la majorité des 346 équipements identifiés comme vulnérables et exposés sur Internet est utilisée dans des installation de production d'énergie et dans des stations d'épuration. L'ANSSI et ACYMA en ont informé leurs propriétaires. Ces équipements particulièrement vulnérables peuvent être manipulés à distance par des attaquants afin de compromettre les réseaux industriels et in fine perturber leurs activités de production. Les utilisateurs de ces systèmes doivent donc vérifier la nécessité de maintenir une accessibilité de ces équipements à distance et, si cela s'avère être le cas, mettre en place les mesures permettant de limiter l'accès à ces équipements par les seuls acteurs ayant besoin de s'y connecter (équipements de filtrage, réseau privé virtuel, lien réseau dédié).
	NUM 51-02 NUM 52-02	Additionnelle	Adapter les dispositifs de réponse à incidents aux caractéristiques de la menace.	Afin de s'assurer d'être en mesure de répondre de manière rapide et efficace à un incident de sécurité informatique, il est nécessaire de construire un dispositif de réponse adéquat. En particulier, l'identification des ressources humaines en mesure d'armer les centres opérationnels de réponse est nécessaire, en passant si besoin par la contractualisation de prestataires de réponse aux incidents de sécurité (PRIS) pour renforcer l'action des équipes internes. En complément, la définition d'une procédure-cadre de gestion des incidents ainsi que de fiches-réflexes pour les scénarios d'attaques les plus pertinents pour l'organisation (chiffrement d'un poste, DDoS, exfiltration de données, etc.) permettent de mettre en œuvre rapidement la réponse à incident, et donc d'en réduire la portée de manière significative. Enfin, les organisations doivent également vérifier qu'un plan de continuité d'activité (PCA), détaillant les besoins de continuité de leur centre opérationnel, existe et puisse

				être mobilisé pour assurer la continuité de la réponse en cas d'incident, même de nature non-cyber (disfonctionnement électrique, télécoms, indisponibilité bâtimentaire, etc.). Les moyens de continuité identifiés via le PCA doivent être vérifiés via des tests et des exercices afin d'assurer de leur parfaite disponibilité et efficacité en cas d'incident les mobilisant.
	NUM 51-05	Additionnelle	Réaliser des tests de restauration des sauvegardes.	Afin de s'assurer de la capacité d'une reprise rapide de l'activité en cas d'attaque destructive et d'entrainer les équipes en charge de ces opérations, il convient d'organiser régulièrement des tests de restauration des sauvegardes réalisées sur les systèmes d'information. Ces tests, qui doivent être effectués sur les sauvegardes en ligne et hors-ligne, sont une opportunité de vérifier la présence des sauvegardes, leur qualité et l'aptitude à restaurer un système d'information à partir de ces dernières. Le guide « d'hygiène numérique » de l'ANSSI apporte des précisions vis-à-vis de la mise en place de politiques de sauvegarde et de réalisation des tests : https://cyber.gouv.fr/publications/guide-dhygiene-informatique
Santé				
	SAN 10-01	Socle	Assurer une veille sanitaire permanente visant à détecter l'utilisation d'un agent NRBC contre la population et une capacité analytique permanente permettant d'identifier un agent NRBC dans le domaine sanitaire.	

	SAN 20-01	Socle	Assurer une capacité permanente de prise en charge de victimes d'actes de terrorisme (blessés ou malades).	Les agences régionales de santé (ARS) veillent, d'une part, à bien articuler le schéma ORSAN AMAVI avec le plan ORSEC des préfectures et, d'autre part, à organiser le dispositif sanitaire des grands événements à sensibilité particulière selon les orientations des préfets.
	SAN 30-01	Socle	Assurer le fonctionnement nominal des chaines de production des produits de santé et l'approvisionnement en matières premières pharmaceutiques au niveau des opérateurs du secteur des produits de santé	
	SAN 30-02	Socle	S'assurer de la permanence des capacités de distribution des produits de santé, équipements et matériels sanitaires.	
	SAN 40-01	Socle	Assurer une sécurisation permanente des établissements de santé et médico-sociaux.	Un effort tout particulier est demandé aux directeurs des établissements de santé qui doivent poursuivre la sécurisation de leurs sites en s'appuyant sur le déploiement de leur plan de sécurité d'établissement (PSE) et la mise en œuvre d'actions de formation à l'intention de l'ensemble de leurs personnels.

Réseaux d'eau				
	EAU 20-04	Socle	Établir, mettre à jour et tester les possibilités de secours, de substitution et d'interconnexion.	
	EAU 20-05	Socle	Organiser le dispositif de veille, d'alerte, d'astreinte, de permanence et de gestion de crise et maintenir le réseau de contacts avec les autorités.	
	EAU 20-06	Socle	Établir, mettre à jour et tester périodiquement les plans d'opération internes (POI), plans particuliers d'intervention (PPI), plans particuliers de protection (PPP) et plans de protection externes (PPE), garantir les capacités d'intervention.	
	EAU 20-10	Socle	Surveiller les points les plus vulnérables	

			du réseau d'alimentation en eau.	
	EAU 20-13	Socle	Mettre en place une astreinte ou une permanence dans les laboratoires des exploitants et les laboratoires agréés en charge du contrôle sanitaire des eaux.	
L'étranger				
	EXT 10-05	Socle	S'inscrire sur Ariane (voyageurs).	Ces mesures de précaution permettent de : - recueillir les numéros utiles, prendre connaissance des consignes de sécurité et les conserver pendant toute la durée d'un séjour à l'étranger ; - recevoir des recommandations de sécurité par courriels si la situation le justifie ; - être contacté en cas de crise dans le pays de destination ; - prévenir, en cas de besoin, la personne contact désignée sur Ariane.