ACADÉMIE
DE CRÉTEIL

Liberté
Égalité
Fraternité

Politique de Sécurité des Systèmes d'Information de l'Académie de Créteil

ANNEXE 2

Référentiel d'exigences de sécurité pour les systèmes d'information des établissements d'enseignement du premier et du second degré

Sommaire

I. Assistance

ORG-ASS1	Assistance aux utilisateurs

Les modalités d'assistance aux utilisateurs sont organisées conjointement entre l'académie et la collectivité.

Ces modalités comportent la qualification, le traitement et le suivi des signalements. Une revue de ces modalités est organisée régulièrement et mesure le niveau de satisfaction utilisateur.

ORG-ASS2	Télé-assistance

L'académie doit pouvoir assurer l'assistance et de la maintenance à distance des équipements ou applications qu'elle prend en charge pour le compte de l'établissement.

II. Traitement des incidents

TI-MOB	Mobilisation en cas d'alerte

En cas d'alerte de sécurité identifiée au niveau national (CERT, ANSSI, COSSIM, MENJ), l'académie s'assure de la bonne application des exigences formulées par les instances nationales, dans les meilleurs délais.

Le RSSI ou son adjoint les transmettent à la collectivité territoriale en responsabilité.

TI-QUAL-TRAIT	Qualification et traitement des incidents

Le RSSI est informé par la chaîne opérationnelle de tout incident de sécurité et contribue si nécessaire à la qualification de l'incident et au pilotage de son traitement.

TI-INC-REM	Remontée des incidents

Les critères et procédures précis de remontée d'incidents sont élaborés sous le pilotage concerté de l'académie et de la collectivité, en lien avec la chaîne opérationnelle.
Un processus identifié de chaîne d'alerte d'incidents de sécurité doit mis en place entre la collectivité et l'académie.
Chaque entité doit maintenir à jour un historique clair des suites liées à l'escalade de chaque incident afin de capitaliser les enseignements associés à la résolution (ou non) de ces incidents.

III. Ressources humaines

RH-SSI	Charte d'application de la SSI
	Une charte d'application des mesures pratiques d'utilisation sécurisée des ressources informatiques propres à l'établissement peut être élaborée par l'entité. Cette charte doit être opposable juridiquement et, si possible, intégrée au règlement intérieur. Le personnel non permanent (stagiaires,contractuels, apprentis, prestataires) est informé de ses devoirs dans le cadre de son usage des SI.
RH-CONF	Personnels de confiance
	Les personnels relevant de l'académie, de l'établissement, de la collectivité, des prestataires, en charge de l'administration des équipements sont des personnes de confiance. Elles manipulent des informations sensibles, et doivent le faire avec une attention et une probité particulière, dans le respect des textes en vigueur. Les sanctions éventuelles s'appliquant aux cas de négligence ou de malveillance leur sont communiquées. Elles doivent en être informées.
RH-UTIL	Sensibilisation des utilisateurs des systèmes d'information
	Chaque utilisateur doit être régulièrement informé des exigences de sécurité le concernant, et motivé à leur respect. Il doit être formé à l'utilisation des outils de travail conformément aux règles de la SSI.
RH-MOUV	Gestion des arrivées, des mutations et des départs
	Une procédure permettant de gérer les arrivées, les mutations et les départs des personnels en charge de l'administration du SI doit être formalisée et appliquée strictement. Cette procédure doit couvrir au minimum : - la gestion et la révocation des comptes et des droits d'accès aux SI, y compris pour les partenaires et les prestataires externes ; - la gestion du contrôle d'accès aux locaux ; - la gestion des équipements mobiles ; - la gestion du contrôle des habilitations. Cette procédure est mise à disposition du RSSI.

IV. Gestion des biens

GDB-QUALIF-SENSI	Qualification des informations
	La sensibilité de toute information doit être évaluée. Le marquage systématique des documents, en fonction du niveau de sensibilité, est fortement recommandé.
GDB-PROT-IS	Protection des informations
	L'utilisateur doit protéger les informations qu'il est amené à manipuler dans le cadre de ses fonctions, selon leur sensibilité et tout au long de leur cycle de vie, depuis la création du brouillon jusqu'à son éventuelle destruction.

V. Intégration de la SSI dans le cycle de vie des systèmes d'information

INT-AQ-PSL	Acquisition de produits de sécurité et de services de confiance
	Lorsqu'ils sont disponibles et qu'ils correspondent au besoin, des produits de sécurité ou des services de confiance labellisés (agréés, qualifiés ou certifiés) par l'ANSSI ou le ministère de tutelle doivent être utilisés.
INT-PRES-CS	Clauses de sécurité
	Toute prestation dans le domaine des SI est encadrée par des clauses de sécurité. Ces clauses spécifient les mesures SSI que le prestataire doit respecter dans le cadre de ses activités.
INT-REX-HB	Localisation de l'hébergement
	L'hébergement sur le territoire national est obligatoire pour les données sensibles de l'administration, sauf accord du RSSI, et dérogation dûment motivée.
INT-REX-HS	Hébergement et clauses de sécurité
	Tout contrat d'hébergement détaillant les dispositions mises en œuvre pour prendre en compte la SSI est soumis pour avis au RSSI. Ce sont notamment les mesures prises pour assurer le maintien en condition de sécurité des systèmes et permettre une gestion de crise efficace (conditions d'accès aux journaux, mise en place d'astreintes, etc.).

VI. Sécurité physique

PHY-PUBL	Accès réseau en zone d'accueil du public
	Tout accès au réseau installé dans une zone d'accueil du public ou depuis un terminal non géré par l'entité doit être filtré ou isolé du reste du réseau informatique de l'entité.
PHY-TECH	Sécurité physique des locaux techniques
	L'accès aux locaux techniques abritant des équipements d'alimentation et de distribution d'énergie ou des équipements de réseau et de téléphonie doit être physiquement protégé.
PHY-CI-CTRLACC	Contrôle d'accès physique
	L'accès aux zones internes (autorisées uniquement au personnel du centre informatique ou aux visiteurs accompagnés) et restreintes (autorisées aux seules personnes habilitées ou aux visiteurs accompagnés) doit reposer sur un dispositif de contrôle d'accès physique. Ce dispositif doit être maintenu en condition de sécurité de façon rigoureuse.
PHY-CI-MOYENS	Délivrance des moyens d'accès physique
	La délivrance des moyens d'accès physique doit respecter un processus formel permettant de s'assurer de l'identité de la personne et s'appuyer sur le processus d'arrivée et de départ du personnel. Le personnel autre que celui explicitement autorisé ou habilité mais néanmoins appelé à intervenir dans les zones internes ou restreintes (entretien ou réparation des bâtiments ou des équipements non informatiques, nettoyage, visiteurs) accède à ces zones sous surveillance permanente et systématique.
PHY-CI-TRACE	Traçabilité des accès
	Une traçabilité des accès des visiteurs externes aux zones restreintes doit être mise en place. Ces traces sont conservées un an, dans le respect de la réglementation protégeant les données personnelles.
PHY-CI-ENERGIE	Local énergie
	L'alimentation de secteur des équipements devra être conforme, de façon à se prémunir contre les atteintes à la sécurité des personnes et des équipements liées à un défaut électrique.

PHY-CI-CLIM	Climatisation

Une climatisation proportionnée aux besoins énergétiques du système informatique doit être installée.
Des procédures de réaction en cas de panne, connues du personnel, doivent être élaborées et vérifiées annuellement.
Ces dispositions visent à prévenir toute surchauffe des équipements, pouvant engendrer une perte du service voire une détérioration du matériel.

VII. Sécurité des réseaux

RES-INTERCO	Interconnexion avec des réseaux externes

Toute interconnexion entre les réseaux locaux d'un établissement et un réseau externe est soumise à l'accord du RSSI.
Cela concerne notamment les réseaux suivant:
- Réseau d'un tiers
- Internet
- Téléphonie sur IP (ToIP)
- Gestion Technique des Bâtiments (GTB)
- Vidéo-Surveillance

RES-ENTSOR	Filtrage réseau pour les flux sortants et entrants.

Dans l'optique de réduire les possibilités offertes à un attaquant, les connexions des machines du réseau interne vers l'extérieur doivent être filtrées.
Les flux entre les différentes zones internes doivent également être filtrés, en respect de la politique de sécurité du réseau RACINE et des recommandations du RSSI académique.

RES-FILTRAGE-WEB	Filtrage des accès au web

Les accès à internet sur les protocoles FTP(S), HTTP(S) sont journalisés et filtrés afin de protéger le SI contre des usages malveillants ou non appropriés.
Les journaux d'accès sont conservés sur douze mois glissants.

RES-PROT	Protection des informations

Les accès à Internet passent obligatoirement à travers des passerelles maîtrisées de l'entité.
Dès lors que des informations sensibles doivent transiter sur des réseaux non maîtrisés, il convient de les protéger spécifiquement par un chiffrement adapté.

RES-CLOIS	Cloisonner le SI en sous-réseaux de niveaux de sécurité homogènes
	Le système d'information doit être segmenté selon des zones présentant chacune un niveau de sécurité homogène. Les réseaux des EPLE sont organisés en zones (zone administrative, zone pédagogique, DMZ). La zone administrative est porteuse des exigences RACINE-AGRIATES. Elle est interconnectée à RACINE.
RES-INTERCOGEO	Interconnexion des sites géographiques locaux d'une entité
	Les zones administratives d'établissements sous la responsabilité juridique d'un même chef d'établissement doivent pouvoir communiquer entre elles de manière sécurisée.
RES-SSFIL	Mise en place de réseaux sans fil
	Une segmentation du réseau doit être mise en place de façon à limiter à un périmètre déterminé les conséquences d'une intrusion depuis la voie radio. Les protocoles d'accès au réseau wifi doivent respecter les recommandations de l'ANSSI (algorithmes de chiffrement, authentification des utilisateurs). La mise en place de réseaux sans fils sur la zone administrative est soumise à accord du RSSI, qui en cas d'accord, définira les exigences nécessaires.
RES-COUCHBAS	Protection contre les attaques sur les couches basses
	Une attention particulière doit être apportée à l'implantation des protocoles de couches basses, de façon à se prémunir des attaques usuelles par saturation ou empoisonnement de cache. Cela concerne, par exemple, le protocole ARP.
RES-ROUTDYN	Surveiller les annonces de routage
	Lorsque l'utilisation de protocoles de routage dynamique est nécessaire, celle-ci doit s'accompagner de la mise en place d'une surveillance des annonces de routage et de procédures permettant de réagir rapidement en cas d'incidents.
RES-SECRET	Modifier systématiquement les éléments d'authentification par défaut des équipements et services
	Les mots de passe par défaut doivent être impérativement modifiés, de même que les certificats. Les dispositions nécessaires doivent être prises auprès des fournisseurs de façon à pouvoir modifier les certificats installés par défaut.

RES-CARTO	Élaborer les documents d'architecture technique et fonctionnelle
	L'architecture en réseau du système d'information doit être décrite et formalisée à travers des schémas d'architecture et des configurations, maintenus au fil des évolutions apportées au SI. Les documents d'architecture sont sensibles et font l'objet d'une protection adaptée. Cette cartographie est mise à disposition du RSSI.
RES-DURCI	Durcir les configurations des équipements de réseaux
	Les équipements de réseaux doivent faire l'objet d'un durcissement spécifique comprenant notamment, outre le changement des mots de passe et certificats, la désactivation des interfaces et services inutiles, ainsi que la mise en place de mécanismes de protection.
RES-FLUX	Routage et priorisation des flux
	La priorisation des flux est réalisée en accord avec l'autorité académique (Services académiques ou chef d'établissement). La priorisation des flux est réalisée en accord avec l'autorité académique (Services académiques ou chef d'établissement).

VIII. Architecture des systèmes d'information

ARCHI-PASS	Passerelles Internet
	Les interconnexions Internet passent obligatoirement par des passerelles de sécurité validées par le RSSI.
ARCHI-LOC-HB	Localisation de l'hébergement
	L'hébergement sur le territoire national est obligatoire pour les données sensibles de l'administration, sauf accord du RSSI, et dérogation dûment motivée.

IX. Exploitation des systèmes d'information

EXP-PROT-INF	Protection des informations sensibles en confidentialité et en intégrité
	Des mesures doivent être mises en œuvre afin de garantir la protection des informations sensibles en termes de confidentialité et d'intégrité. A défaut d'utilisation d'un réseau homologué, ces informations doivent être chiffrées à l'aide d'un moyen de chiffrement labellisé.

EXP-TRAC	Traçabilité des interventions sur le système
	Les interventions de maintenance sur les ressources informatiques de l'entité doivent être tracées. Les traces doivent être accessibles durant au moins un an.
EXP-CONFIG	Configuration des ressources informatiques
	Les systèmes d'exploitation et les logiciels doivent faire l' objet d'un durcissement. Les configurations et les mises à jour sont effectuées dans le strict respect des guides ou des procédures en vigueur dans l'académie ou, à défaut, en vigueur au niveau du ministère ou de l'ANSSI.
EXP-ID-AUTH	Identification, authentification et contrôle d'accès logique
	L'accès à toute ressource non publique doit nécessiter une identification et une authentification individuelle de l'utilisateur. Dans le cas de l'accès à des données sensibles, des moyens d'authentification forte doivent être utilisés. Le contrôle d'accès doit être géré et s'appuyer sur un processus formalisé cohérent avec la gestion des ressources humaines.
EXP-PROC-AUTH	Autorisations d'accès des utilisateurs
	Toute action d'autorisation d'accès d'un utilisateur à une ressource des SI doit s'inscrire dans le cadre d'un processus d'autorisation formalisé, qui s'appuie sur le processus d'arrivée et de départ du personnel.
EXP-REVUE-AUTH	Revue des autorisations d'accès
	Une revue des autorisations d'accès doit être réalisée annuellement sous le contrôle du RSSI, le cas échéant avec l'appui du correspondant local de la SSI.
EXP-CONF-AUTH	Confidentialité des informations d'authentification
	Les informations d'authentification (mots de passe d'accès aux SI, clés privées liées aux certificats électroniques, etc.) doivent être considérées comme des données sensibles.
EXP-GEST-PASS	Gestion des mots de passe
	Les utilisateurs ne doivent pas stocker leurs mots de passe en clair, par exemple dans un fichier, sur leur poste de travail. Les mots de passe ne doivent de préférence pas transiter en clair sur les réseaux, sauf si le réseau est suffisamment cloisonné et sécurisé.

EXP-INIT-PASS	Initialisation des mots de passe
	Chaque compte utilisateur doit être créé avec un mot de passe initial aléatoire unique. Si les circonstances l'imposent, un mot de passe plus simple mais à usage unique peut être envisagé.
EXP-SEQ-ADMIN	Séquestre des authentifiants des administrateurs
	Les authentifiants permettant l'administration des ressources des SI doivent être placés sous séquestre et tenus à jour, dans un coffre ou une armoire fermée à clé ou stockées dans un logiciel sécurisé.
EXP-POL-ADMIN	Politique de mots de passe « administrateurs »
	Chaque administrateur doit disposer d'un identifiant avec mot de passe propre et destiné à l'administration avec un niveau de privilèges de type super-utilisateur. Le compte root ne doit pas être utilisé.
EXP-DEP-ADMIN	Gestion du départ d'un administrateur des SI
	En cas de départ d'un administrateur disposant de privilèges sur des composants des SI, les comptes individuels dont il disposait doivent être immédiatement désactivés. Les éventuels mots de passe d'administration dont il avait connaissance doivent être changés, par exemple les mots de passe des comptes fonctionnels, des comptes génériques ou des comptes de service utilisés dans le cadre des fonctions de l'administrateur.
EXP-HABILIT-ADMIN	Habilitation des administrateurs
	L'habilitation des administrateurs (de l'académie, de l'établissement, de la collectivité, des prestataires) s'effectue selon une procédure validée par le responsable hiérarchique. La procédure d'habilitation et le nombre de personnes habilitées sont tenus à disposition du RSSI académique.
EXP-PROT-ADMIN	Protection des accès aux outils d'administration
	L'accès aux outils et aux interfaces d'administration doit être strictement limité aux personnes habilitées.
EXP-GEST-ADMIN	Gestion des actions d'administration
	Les opérations d'administration sur les composants techniques liés à la sécurité doivent être tracées de manière à pouvoir gérer au niveau individuel leur imputabilité.

EXP-RESTR-DROITS	Restriction des droits
	Sauf exception dûment motivée et validée par le RSSI, les utilisateurs n'ont pas de droits d'administration.
EXP-SECX-DIST	Sécurisation des outils de prise de main à distance
	Des mesures de sécurité spécifiques doivent être définies et respectées pour la prise en main à distance. Ces mesures intègrent le consentement des utilisateurs et sont tenues à disposition du RSSI.
EXP-SEC-FLUX-ADMIN	Sécurisation des flux d'administration
	Les opérations d'administration sur les ressources locales d'un établissement doivent s'appuyer sur des protocoles sécurisés, mettant en œuvre du chiffrement.
EXP-MAINT-EXT	Maintenance externe
	Les données non chiffrées doivent être effacées avant l'envoi en maintenance externe de toute ressource informatique, sauf si elle sont chiffrées à l'aide de produits de sécurité validés par le RSSI. L'effacement des données sensibles doit s'appuyer sur des produits validés par le RSSI.
EXP-MIS-REB	Mise au rebut
	Lorsqu'une ressource informatique est amenée à quitter définitivement l'entité, les données présentes sur les disques durs ou la mémoire intégrée doivent être effacées de manière sécurisée à l'aide de produits de sécurité qualifiés par l'ANSSI.
EXP-PROT-MALV	Protection contre les codes malveillants
	Des logiciels de protection contre les codes malveillants, appelés communément antivirus, doivent être installés sur l'ensemble des serveurs d' interconnexion, des serveurs applicatifs et des postes de travail de l'entité.
EXP-GES-ANTIVIR	Gestion des événements de sécurité de l'antivirus
	Les événements de sécurité de l'antivirus doivent être supervisés pour une gestion des problèmes a posteriori (exemples : serveur constamment infecté, virus détecté et non éradiqué par l'antivirus, etc.).
EXP-MAJ-ANTIVIR	Mise à jour de la base de signatures
	Les mises à jour des bases antivirales et des moteurs d'antivirus doivent être déployées automatiquement sur les serveurs et les postes de travail.

EXP-NAVIG	Configuration du navigateur Internet
	Les navigateurs déployés sur l'ensemble des serveurs et des postes de travail nécessitant un accès Internet ou Intranet doit être configuré de manière sécurisée en respectant au maximum les recommandations de l'ANSSI.
EXP-POL-COR	Définir et mettre en œuvre une politique de suivi et d'application des correctifs de sécurité.
	Le maintien du niveau de sécurité d'un système d'information impose une gestion organisée et adaptée des mises à jour de sécurité. Un processus de gestion des correctifs propre à chaque système ou applicatif doit être défini et adapté aux contraintes et au niveau d'exposition du système.
EXP-OBSOLET	Assurer la migration des systèmes obsolètes
	L'ensemble des logiciels utilisés sur le système d'information doit l'être dans une version pour laquelle l'éditeur assure le support et le tient à jour. En cas de défaillance du support, il convient d'en étudier l'impact et de prendre les mesures adaptées.
EXP-ISOL	Isoler les systèmes obsolètes restants
	Il est nécessaire d'isoler les systèmes obsolètes, qui sont gardés volontairement pour assurer un maintien en condition opérationnelle des projets et pour lesquels une migration n'est pas envisageable. Chaque fois que cela est possible, cette isolation doit être effectuée au niveau du réseau par un filtrage strict, au niveau des éléments d'authentification, qui ne doivent pas être communs avec le reste du SI, et au niveau des applications (aucune ressource ne doit être partagée avec le reste du SI).
EXP-JOUR-SUR	Journalisation des alertes
	Chaque système doit disposer de dispositifs de « journalisation » permettant de conserver une trace des événements de sécurité. Ces traces doivent être conservées de manière sûre et accessibles au RSSI.
EXP-CONS-JOUR	Conservation des journaux
	Les journaux des événements de sécurité doivent être conservés pendant douze mois glissants, hors contraintes légales et réglementaires particulières imposant des durées de conservation spécifiques.

EXP-GES-DYN	Gestion dynamique de la sécurité
	L'académie et la collectivité procèdent conjointement, notamment via l'analyse des journaux, à la surveillance des comportements anormaux au sein du système d'information et à la surveillance des flux d'entrée et de sortie du système d'information.
EXP-DECLAR-VOL	Déclarer les pertes et vols
	Toute perte ou vol d'une ressource d'un système d'information doit être déclarée au RSSI
EXP-CI-OS	Systèmes d'exploitation
	Les systèmes d'exploitation déployés doivent faire l'objet d'un support valide de la part d'un éditeur ou d'un prestataire de service. Les systèmes ne pouvant être mis à jour pour des raisons de compatibilité applicative doivent faire l'objet de mesures de sécurité renforcées.
EXP-CI-PROTFIC	Passerelle d'échange de fichiers
	Les échanges de fichiers entre applications doivent privilégier les protocoles sécurisés (SSL/TLS, FTPS, etc.).
EXP-CI-FILT	Filtrage des flux applicatifs
	De façon à garantir un niveau de sécurité satisfaisant face aux attaques informatiques, des mécanismes de filtrage et de cloisonnement doivent être mis en œuvre.
EXP-CI-EFFAC	Effacement de support
	Le reconditionnement et la réutilisation des disques durs pour un autre usage, par exemple la réattribution d'une machine ou d'un serveur, ne sont autorisés qu'après une opération d'effacement sécurisé des données.
EXP-CI-TRAC	Traçabilité et imputabilité
	Afin d'assurer une cohérence dans les échanges entre applications ainsi qu'une traçabilité pertinente des événements techniques et de sécurité, les centres d'exploitation emploient une référence de temps commune (service NTP, Network Time Protocol).
EXP-CI-PI	Protection des services exposés sur l'internet
	La publication sur Internet de services hébergés par l'établissement doit se faire au travers d'un service mandataire inversé avec un protocole sécurisé (TLS).

EXP-CI-DNS	Service de noms de domaine - DNS technique
	Dans le cas du déploiement d'un serveur de noms de domaines pour les besoins techniques internes les extensions sécurisées DNSSEC sont utilisées.
EXP-CI-ACCRES	Accès aux réseaux
	Le contrôle physique des accès réseaux, l'attribution des adresses IP, le filtrage des informations et l'usage de dispositifs spécifiques (machines virtuelles, cartes d'administration à distance, etc.) font l'objet de procédures sécurisées. Ces procédures sont tenues à disposition du RSSI académique.
EXP-CI-AUDIT	Audit/contrôle
	L'académie peut engager des audits à la demande des chefs d'établissements, de la collectivité, du ministère, de l'ANSSI ou de sa propre autorité pour s'assurer de la conformité aux exigences.

X. Sécurité du poste de travail

PDT-RES-ADM	Poste de travail administratif
	Les postes de travail des établissements, identifiés comme administratifs et devant communiquer avec le réseau RACINE doivent le faire de façon sécurisée. Ils doivent répondre à des exigences de configuration définies dans une procédure dédiée.
PDT-CHIFF-SENS	Chiffrement des données sensibles
	Un moyen de chiffrement labellisé doit être mis à la disposition des utilisateurs et des administrateurs afin de chiffrer les données sensibles stockées sur les postes de travail, les serveurs, les espaces de travail ou les supports amovibles.
PDT-NOMAD-STOCK	Stockage local d'information sur les postes nomades
	Les informations sensibles stockées sur les postes nomades doivent être obligatoirement chiffrées par un moyen de chiffrement approuvé par le RSSI.

PDT-MUL-DURCISS	Durcissement des imprimantes et des copieurs multifonctions
	Les imprimantes et les copieurs multifonctions hébergés localement dans une entité doivent faire l'objet d'un durcissement en termes de sécurité : changement des mots de passe initialement fixés par le constructeur, chiffrement des données sur le disque dur lorsque cette fonctionnalité est disponible, configuration de réseau statique.
PDT-MUL-SECNUM	**Sécurisation de la fonction de numérisation**
	Lorsqu'elle est activée, la fonction de numérisation sur les copieurs multifonctions hébergés dans une entité doit être sécurisée. Les mesures de sécurité suivantes doivent notamment être appliquées : envoi de documents uniquement à destination d'une adresse de messagerie interne à l'entité, envoi à une seule adresse de messagerie.

XI. Filtrage web

FILT-WEB-AUTH-INT	Authentification des accès vers internet depuis l'établissement ou l'école
	Toute activité vers l'internet initiée au sein de l'établissement ou de l'école doit faire l'objet d'une authentification directe ou indirecte de l'utilisateur. Sont concernés tous les terminaux connectés physiquement ou par Wi-Fi au réseau local.
FILT-WEB-AUTH-EXT	Authentification des accès vers internet depuis l'extérieur de l'établissement ou l'école
	Toute activité vers l'internet depuis un terminal fourni par la collectivité ou l'académie doit faire l'objet d'une authentification directe ou indirecte de l'utilisateur.
FILT-WEB-TRAC	Traçage des activités vers l'internet
	Toute activité vers l'internet depuis un terminal fourni par la collectivité ou l'académie doit être tracée. Ces traces doivent être accessibles aux chefs d'établissements et au RSSI académique. Elle sont conservées durant un an.
FILT-WEB-REVUE	Revue des navigations
	Le contrôle à posteriori des informations consultées sur internet doit être accessible sur réquisition judiciaire ou sur demande du RSSI.
FILT-WEB-MIN-CONT	Contrôle des navigations des mineurs
	Un contrôle des navigations internet initiées par les élèves est effectué, en interdisant l'accès à un ensemble de sites reconnus comme inappropriés au sens de la circulaire 2004-035 du 18 février 2004 par l'intermédiaire de mécanismes adaptés réputés efficaces tels que listes noires, listes blanches et analyse sémantique des réponses aux requêtes HTTPS, contrôle des requêtes des moteurs de recherche d'images, etc. Ce contrôle s'applique pour tout terminal fourni par la collectivité ou l'académie situé à l'intérieur et à l'extérieur de l'établissement ou de l'école.
FILT-WEB-MIN-ADMIN	Ajustement du contrôle de navigation des mineurs
	Les déploiements d'accès à l'internet dans le cadre pédagogique doivent s'effectuer en prenant en compte les besoins des équipes éducatives. Le chef d'établissement , l'IEN du 1er degré ou le directeur d'école doit pouvoir activer ou désactiver certains services, paramétrer les règles de filtrage. Ces modifications peuvent être obtenues sur demande auprès de la collectivité ou être effectuées à partir d'interfaces d'administration délégables.

FILT-WEB-MIN-PROFILS	Profils de filtrage
	Le paramétrage des règles de filtrage doit pouvoir prendre en compte les différents acteurs ou groupes, les flux de données, les applications, les différentes zones, les postes, et les plages horaires.
FILT-WEB-MIN-ALERTE	Signalement d'incident
	Tout incident, notamment lié à l'accessibilité de pages inappropriées, est signalé à la chaîne d'alerte académique. Ceci permet d'engager les mesures adaptées dans les meilleurs délais et d'assurer la circulation de l'information utile au maintien du niveau de protection optimal.
FILT-WEB-MIN-ACTION	Filtrage d'urgence
	Le RSSI peut, s'il estime la situation critique, commanditer la mise en œuvre d'une configuration de filtrage adaptée sur l'ensemble des passerelles du périmètre académique.