ACADÉMIE
DE VERSAILLES
Liberté
Égalité
Fraternité

L'ACADÉMIE
vous accompagne

POLITIQUE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION DE L'ACADÉMIE DE VERSAILLES

ANNEXE 2

RÉFÉRENTIEL D'EXIGENCES DE SÉCURITÉ POUR LES SYSTÈMES D'INFORMATION DES ÉTABLISSEMENTS D'ENSEIGNEMENT DU PREMIER ET DU SECOND DEGRÉ

Sommaire

Glossaire

SI : système d'information

SSI : sécurité des systèmes d'information

RSSI : responsable de la sécurité des systèmes d'information

ANSSI : agence nationale de la sécurité des systèmes d'information

DMZ : demilitarized zone

TLS : protocole de chiffrement « Tertiary Lymphoid Structure »

DNSSEC : protocole sécurisé « Domain Name System Security Extensions »

ARP : Address Resolution Protocol

HTTPS : Hypertext Transfert Protocol Secured

RACINE : Réseau d'Accès et de Consolidation des Intranets de l'Éducation

EPLE : établissement public local d'enseignement

IEN : inspecteur de l'éducation nationale

Assistance

CODE	*TITRE*	*DESCRIPTION*
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.

Traitement des incidents

CODE	*TITRE*	*DESCRIPTION*
TI-MOB	Mobilisation en cas d'alerte	En cas d'alerte de sécurité identifiée au niveau national, l'académie transmet les exigences formulées par les instances nationales à la collectivité territoriale, dans les meilleurs délais et s'assure de leur bonne application.
TI-QUAL-	Qualification et traitement des	L'académie est informée par la chaîne opérationnelle de tout incident de sécurité et contribue si nécessaire à la qualification de

TRAIT	incidents	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.
TI-INC-REM 3	Historique des incidents	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.

Ressources humaines

CODE	*TITRE*	*DESCRIPTION*
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 particulières, 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-MOUV	Gestion des arrivées, des mutations et des départs	Une procédure permettant de gérer les arrivées, les mutations et les départs des personnes (de l'académie, de l'établissement, de la collectivité, des prestataires) en charge de l'administration des équipements doit être formalisée, et appliquée strictement. Cette procédure doit couvrir la gestion/révocation des comptes et des droits d'accès, y compris pour les prestataires externes et la gestion du contrôle des habilitations. Cette procédure est mise à disposition de l'AQSSI.

Sécurité physique

CODE	*TITRE*	*DESCRIPTION*
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, des équipements de réseau et de téléphonie ou des serveurs 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-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-CLIM	Climatisation	Une climatisation proportionnée aux besoins énergétiques du système informatique doit être installée. Ces dispositions visent à prévenir toute surchauffe des équipements, pouvant engendrer une perte du service voire une détérioration du matériel.

Réseaux

CODE	***TITRE***	***DESCRIPTION***
RES-INTERCO1	Interconnexion avec des réseaux externes	Toute interconnexion entre les réseaux locaux d'un établissement et un réseau externe (réseau d'un tiers, Internet, téléphonie sur IP, gestion technique des bâtiments, etc.) est soumise à l'accord de l'AQSSI. La collectivité territoriale saisit le RSSI académique préalablement à tout changement sur l'architecture de l'infrastructure réseau de l'établissement.
RES-INTERCO2	Postes administratifs	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.
RES-INTERCO3	Zones administratives d'établissements	Les zones administratives d'établissements sous la responsabilité juridique d'un même chef d'établissement doivent pouvoir communiquer entre elles de manière sécurisée.
RES-ENTSOR	Filtrage des flux réseaux	Dans l'optique de réduire les possibilités offertes à un attaquant, les connexions des machines du réseau interne vers l'extérieur doivent être filtrées en entrée et en sortie. 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-CLOIS	Cloisonnement du SI en sous-réseaux	Par analogie avec le cloisonnement physique d'un bâtiment, 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 privée, DMZ publique). La zone administrative est porteuse des exigences RACINE. Elle est interconnectée à RACINE.
RES-SSFIL1	Mise en place de réseaux sans fil	En cas de déploiement de réseaux sans fil et en raison de leurs protections intrinsèques insuffisantes, des mesures complémentaires, doivent être prises dans le cadre de la défense en profondeur. En particulier, 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 flux doivent être chiffrés avec des algorithmes validés par l'ANSSI. Les utilisateurs doivent être authentifiés.
RES-SSFIL2	Mise en place de réseaux sans fils sur la zone administrative	La mise en place de réseaux sans fils sur la zone administrative est soumise à accord du RSSI académique, 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	Surveillance des annonces de routage	Lorsque l'utilisation de protocoles de routage dynamiques 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	Authentification par défaut sur les équipements et services	Les mots de passe par défaut doivent être impérativement modifiés, de même en ce qui concerne les certificats. Les dispositions nécessaires doivent être prises auprès des fournisseurs d'équipements de façon à pouvoir modifier les certificats installés par défaut.
RES-DURCI	Durcir les configurations des équipements de réseaux	Les équipements de réseaux (tel que les routeurs) 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-CARTO	Documentation des architectures réseau	L'architecture 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. La cartographie réseau s'insère dans la cartographie globale des SI. Cette cartographie est mise à

		disposition du RSSI académique.
RES-FLUX1	Priorisation des flux	La priorisation des flux est réalisée en accord avec l'autorité académique (Services académiques ou chef d'établissement).
RES-FLUX2	Routage des flux internet des postes administratifs	Les flux vers Internet des postes des EPLE identifiés comme administratifs ne remontent pas vers le réseau RACINE.

Architecture technique

CODE	*TITRE*	*DESCRIPTION*
ARCHI-PASS	Passerelles Internet	Les interconnexions Internet passent obligatoirement par des passerelles de sécurité validées par le RSSI académique.
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.

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

CODE	*TITRE*	*DESCRIPTION*
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 détaille les dispositions mises en œuvre pour prendre en compte la SSI. 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.). Le RSSI émet un avis après analyse des documents fournis.

Exploitation

CODE	*TITRE*	*DESCRIPTION*
EXP-TRAC	Traçabilité des interventions sur le système	Les interventions de maintenance sur les équipements doivent être tracées. Ces traces doivent être accessibles à la personne juridiquement responsable durant un an.
EXP-CONFIG	Configuration des ressources informatiques	Exception faite d'impératifs applicatifs, les mises à jour de sécurité sont appliquées dans les meilleurs délais. Les configurations doivent être ajustées pour garantir la meilleure sécurisation.
EXP-PROFILS	Profils d'accès aux applications d'administration des systèmes	Les applications manipulant des données, telles que celles liées à l'administration des systèmes, doivent permettre une gestion fine par profils d'accès. Les principes du besoin d'en connaître et du moindre privilège s'appliquent.
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.
EXP-REVUE-AUTH	Revue des autorisations d'accès	Une revue des autorisations d'accès doit être réalisée a minima annuellement sous le contrôle du RSSI académique, le cas échéant avec l'appui du correspondant local 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-SAQ-ADMIN	Séquestre des authentifiants « administrateur »	Les authentifiants permettant l'administration des équipements doivent être placés sous séquestre et tenus à jour, dans un coffre, une armoire fermée à clé ou un coffre-fort électronique. Tout accès d'administration à une ressource informatique doit pouvoir être tracé et permettre de remonter à la personne exerçant ce droit. Les informations d'authentification bénéficiant d'un moyen de protection physique n'ont, par défaut, pas besoin d'être l'objet d'opérations de séquestre de la part d'autres personnels que l'authentifié lui-même.
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	En cas de départ d'un administrateur, les comptes individuels dont il disposait doivent être immédiatement désactivés. Les éventuels mots de passe d'administration dont il avait connaissance doivent être changés (exemples : mots de passe des comptes fonctionnels, comptes génériques ou comptes de service utilisés dans le cadre des fonctions de l'administrateur).
EXP-PROT-ADMIN	Protection des accès aux outils d'administration	L'accès aux outils et interfaces d'administration doit être strictement limité aux personnes habilitées, selon une procédure formelle d'autorisation d'accès.
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-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-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-SECX-DIS	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 académique.
EXP-MAINT-EX	Maintenance externe	Les données non chiffrées doivent être effacées de manière sécurisée avant l'envoi de toute ressource informatique en maintenance externe.
EXP-MIS-REB	Mise au rebut	Lorsqu'une ressource informatique est amenée à quitter définitivement l'établissement, les données présentes sur les disques durs ou la mémoire intégrée doivent être effacées de manière sécurisée. L'effacement des données sensibles doit s'appuyer sur des produits qualifiés, ou respecter des procédures établies en concertation avec l'ANSSI.
EXP-POL-COR	Suivi des correctifs de sécurité d'applications	Le maintien dans le temps du niveau de sécurité des composants techniques liés à la sécurité 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 suivant les contraintes et le niveau d'exposition du système.

EXP-OBSOLET	Assurer la migration des systèmes obsolètes	L'ensemble des logiciels utilisés sur les composants techniques liés à la sécurité doit être dans une version pour laquelle l'éditeur assure le support, et tenu à jour. En cas de défaillance du support, il convient d'en étudier l'impact et de prendre les mesures adaptées de façon concertée avec les différentes parties.
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 académique.
EXP-POL-JOUR	Traces et journaux	Une politique de gestion et d'analyse des journaux de traces des événements de sécurité est définie conjointement par l'académie et la collectivité et mise en œuvre. Le niveau de sécurité d'un système d'information dépend en grande partie de la capacité de ses exploitants et administrateurs à détecter les erreurs, dysfonctionnements et tentatives d'accès illicites survenant sur les éléments qui le composent.
EXP-CONS-JOUR	Conservation des journaux	Les journaux des événements de sécurité doivent être conservés sur 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 définissent conjointement les modalités de surveillance des comportements anormaux.
EXP-DECLAR-VOL	Déclarer les pertes et vols	Toute perte ou vol d'une ressource d'un système d'information doit être déclaré au RSSI académique sans délai.
EXP-CI-OS	Systèmes d'exploitation	Les systèmes d'exploitation déployés sur les composants techniques liés à la sécurité doivent faire l'objet d'un support valide de la part d'un éditeur ou d'un prestataire de service. Seuls les services et applications nécessaires sont installés, de façon à réduire la surface d'attaque. Une attention particulière doit être apportée aux comptes administrateurs.
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-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	Dans le cas du déploiement d'un serveur de noms de domaines pour les besoins techniques internes les

	technique	extensions sécurisées DNSSEC sont utilisées.
EXP-CI-EFFAC	Effacement de support	Le reconditionnement et la réutilisation des disques durs pour un autre usage (ex : réattribution d'une machine/serveur) ne sont autorisés qu'après une opération d'effacement sécurisé des données.
EXP-CI-TRAC	Traçabilité / 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-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.

Filtrage web

CODE	*TITRE*	*DESCRIPTION*
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. Elles sont conservées durant un an.
FILT-WEB-REVUE	Revue des navigations	Le contrôle a posteriori des informations consultées sur internet doit être accessible sur réquisition judiciaire ou sur demande du RSSI académique.

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 académique 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.