ACADÉMIE
DE CRÉTEIL

Liberté
Égalité
Fraternité

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

ANNEXE 1

Référentiel d'exigences de sécurité pour les systèmes d'information des services académiques

Sommaire

Référentiel d'exigences de sécurité pour les systèmes d'information des services académiques....1
I. Politique, organisation et gouvernance....3
II. Traitement des incidents....4
III. Ressources humaines....5
IV. Gestion des biens....7
V. Intégration de la SSI dans le cycle de vie des systèmes d'information....8
VI. Sécurité physique....9
VII. Sécurité des réseaux....11
VIII. Architecture des systèmes d'information....13
IX. Exploitation des systèmes d'information....13
X. Sécurité du poste de travail....21
XI. Sécurité du développement des systèmes....23

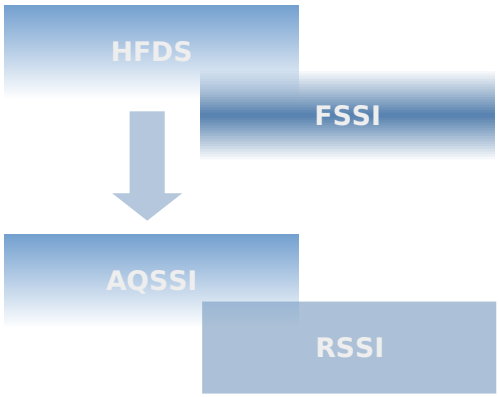
I. Politique, organisation et gouvernance

ORG-SSI	Organisation de la SSI

Une organisation dédiée à la SSI est déployée au sein d'Académie suivant les principes de l'IGI 1300. Cette organisation, établie selon les directives du HFDS, définit les responsabilités internes et à l'égard des tiers, les modalités de coordination avec les autorités externes, ainsi que les modalités d'application des mesures de protection. Des procédures d'applications sont écrites et portées à la connaissance de tous.

ORG-ACT-SI	Identification des acteurs SSI

L'organisation SSI d'Académie s'appuie sur des acteurs SSI clairement identifiés à tous les niveaux. Les acteurs responsables en matière de SSI pour la protection du secret de la défense désignés dans l'IGI 1300, et les agents chargés de les assister dans cette mission, sont responsables de la mise en application générale de la politique SSI locale. Ils sont référencés dans un annuaire local. Cette chaîne fonctionnelle s'appuie, sur le HFDS, assisté par un FSSI.



ORG-RSSI	Désignation du responsable de la SSI

Chaque autorité qualifiée en sécurité des systèmes d'information (AQSSI : Recteur) s'appuie sur un ou plusieurs responsables de la sécurité des systèmes d'information (RSSI), chargé(s) de l'assister dans le pilotage et la gestion de la SSI. Des « correspondants locaux SSI » peuvent être désignés, le cas échéant, afin de constituer un relais du RSSI. Le RSSI ait valider les mesures d'application de la PSSI-A par l'AQSSI et veille à leur application.

ORG-RESP	Formalisation des responsabilités

Le RSSI propose une note d'organisation qui fixe la répartition au sein de chaque entité et au niveau local des responsabilités et rôles en matière de SSI.

ORG-TIERS	Gestion contractuelle des tiers
	Le RSSI coordonne les actions permettant l'intégration des clauses liées à la SSI dans tout contrat ou convention impliquant un accès par des tiers à des informations ou à des ressources informatiques.
ORG-PIL-PSSIM	Définition et pilotage de la PSSI-A
	Chaque Académie établit une politique SSI locale, sous la responsabilité de l'AQSSI. Cette politique reprend le socle commun établi par la PSSI-E ou PSSI-MENJ. Une structure de pilotage de la PSSI locale est définie. Cette structure est chargée de sa mise en place, de son évolution, de son suivi et de son contrôle.
ORG-APP-INSTR	Application de l'instruction dans l'entité
	Le RSSI planifie les actions d'application de la PSSI-A. Il rend compte régulièrement de l'application des mesures de sécurité auprès du FSSI et de l'AQSSI.
ORG-APP-DOCS	Formalisation de documents d'application
	Le RSSI établit et tient à jour les documents permettant l'application des mesures de la PSSI-A.

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), le RSSI s'assure de la bonne application des exigences formulées par les instances nationales, dans les meilleurs délais.
TI-QUAL-TRAIT	Qualification et traitement des incidents
	La chaîne fonctionnelle de la SSI est informée 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
	Tout incident de sécurité, même apparemment mineur, dont l'impact dépasse ou est susceptible de dépasser le périmètre de l'académie, fait l'objet d'un compte-rendu, via la chaîne SSI, au COSSIM du ministère de tutelle. - La remontée d'incidents par les chaînes opérationnelles participe à la posture permanente de vigilance. Cette remontée est immédiate pour les incidents dont la portée est susceptible de dépasser à court terme le

périmètre de l'Académie et pour les incidents correspondant à des signalements spécifiques, notamment de la part de l'ANSSI ou du CERT-RENATER. Les remontées faites au RSSI National prennent la forme d'un buletin mensuel du RSSI Académique pour les autres incidents.
- Les critères et procédures précis de remontée d'incidents sont élaborés sous le pilotage de la chaîne fonctionnelle SSI, en lien avec la chaîne opérationnelle.
- 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.
- L'aspect difficile de la caractérisation des attaques (ambiguïté de la source, du dommage, du moyen, de la finalité) rend nécessaire les échanges d'informations - même sur des « signaux faibles » - ainsi que la coordination continue des actions.

TI-INC-REM 3	Historique des incidents

L'équipe en charge de la SSI maintient un historique précis des suites de chaque incident, afin de capitaliser les enseignements tirés de la résolution ou non de ces incidents.

III. Ressources humaines

RH-SSI	Charte d'application de la SSI

Une charte d'application de la PSSI-A récapitulant les mesures pratiques d'utilisation sécurisée des ressources informatiques et élaborée sous le pilotage de la chaîne fonctionnelle de la SSI, est communiquée à l'ensemble des agents.
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-MOTIV	Choix et sensibilisation des personnes tenant les postes clés de la SSI

Une attention particulière doit être portée au recrutement des personnes clés de la SSI : RSSI, correspondants locaux de la SSI et administrateurs de sécurité.
Les RSSI et leurs correspondants locaux doivent être spécifiquement formés à la SSI.
Les administrateurs des SI doivent être régulièrement sensibilisés aux devoirs liés à leur fonction et doivent veiller à respecter ces exigences dans le cadre de leurs activités quotidiennes.

RH-CONF	Personnels de confiance
	Toutes les personnes manipulant des informations sensibles doivent le faire avec une attention particulière, dans le respect des textes en vigueur. Les sanctions éventuelles s'appliquant aux cas de négligence ou de malveillance leur sont rappelées.
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 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.
RH-NPERM	Gestion du personnel non permanent Stagiaires, contractuels, apprentis, prestataires
	Les règles de la PSSI-A s'appliquent à tout personnel non permanent utilisateur du SI. Les dispositions contractuelles préexistantes régissant l'emploi de ce personnel sont amendées si nécessaire. Pour tout personnel non permanent, un tutorat par un agent permanent est mis en place, afin de l'informer de ces règles et d'en contrôler l'application.

IV. Gestion des biens

GDB-INVENT	**Inventaire des ressources informatiques**

Chaque entité établit et maintient à jour un inventaire des ressources informatiques sous sa responsabilité, en s'appuyant sur un outillage adapté.

Cet inventaire est tenu à la disposition du RSSI académique, du FSSI et de l'ANSSI en cas de besoin de coordination opérationnelle.

Il comprend la liste des « briques » matérielles et logicielles utilisées ainsi que leurs versions exactes.

Il est constitué d'une base de données de configuration, maintenue à jour et tenue à disposition du RSSI.

L'historique des attributions des biens inventoriés doit être conservé, dans le respect de la législation.

GDB-CARTO	**Cartographie**

La cartographie précise les centres informatiques, les architectures des réseaux, sur lesquelles sont identifiés les points névralgiques et la sensibilité des informations manipulées, et qualifie le niveau de sécurité attendu. Cette cartographie est maintenue à jour et tenue à disposition du RSSI académique, du FSSI du ministère et de l'ANSSI en cas de besoin de coordination opérationnelle.

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-HOMOLOG-SSI	**Homologation de sécurité des systèmes d'information**

Le RSSI ou son adjoint sélectionne les systèmes d'information et applications qui doivent faire l'objet d'une analyse de sécurité, en fonction de leur sensibilité.
Cette analyse prend la forme d'un avis ou d'une décision d'homologation.

L'homologation est l'acte selon lequel une autorité, dite autorité d'homologation, désignée par l'AQSSI, atteste formellement auprès des utilisateurs que le système d'information est protégé conformément aux objectifs de sécurité fixés.

La décision d'homologation est prise le cas échéant après avis d'une commission d'homologation.Cette décision s'appuie sur une analyse de risques adaptée aux enjeux du système considéré et précise les conditions d'emploi.

INT-SSI	**Intégration de la sécurité dans les projets**

La sécurité des systèmes d'information doit être prise en compte dans toutes les phases des projets informatiques, sous le contrôle du RSSI, de la conception et de la spécification du système jusqu'à son retrait du service.

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-AR	**Analyse de risques**

Toute opération d'externalisation s'appuie sur une analyse de risques préalable, de façon à déterminer des objectifs de sécurité et définir des mesures adaptées.
L'ensemble des objectifs de sécurité ainsi déterminés permet de définir une cible de sécurité servant de cadre au contrat établi avec le prestataire.

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.).

VI. Sécurité physique

PHY-ZONES	Découpage des sites en zones de sécurité
	Un découpage du centre informatique en zones physiques de sécurité doit être effectué. Des règles doivent fixer les conditions d'accès à ces différentes zones.
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-TELECOM	Protection des câbles électriques et de télécommunications
	Les panneaux de raccordements et les salles des câbles doivent être placés en dehors des zones d'accueil du public et leur accès doit être contrôlé.
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 aux règles de l'art, 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.
PHY-CI-INC	Lutte contre l'incendie
	L'installation de matériel de protection contre le feu est obligatoire. Des procédures de réaction à un incendie sont définies et régulièrement testées.

VII. Sécurité des réseaux

RES-MAITRISE	Systèmes autorisés sur le réseau
	Seuls les équipements gérés et configurés par les équipes informatiques habilitées peuvent être connectés au réseau local d'une entité, à l'exception des équipements personnels des enseignants et de tout autre équipement personnel s'ils sont cloisonnées dans un sous-réseau ne permettant pas d'accéder aux ressources locales.

RES-INTERCO	Interconnexion avec des réseaux externes
	Toute interconnexion entre les réseaux locaux d'une entité et un réseau externe (réseau d'un tiers, Internet, etc.) doit être réalisée via les infrastructures nationales.

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.

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 utilisateurs peuvent demander au RSSI un avis pour lever une interdiction. 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.

RES-INTERCOGEO	Interconnexion des sites géographiques locaux d'une entité
	L'interconnexion au niveau local de réseaux locaux d'une entité n'est possible que si la proximité géographique le justifie et sous réserve de la mise en place de connexions spécifiques et de passerelles sécurisées.

RES-RESS	Cloisonnement des ressources en cas de partage de locaux
	Dans le cas où une entité partage des locaux avec des entités externes, des mesures de cloisonnement des ressources informatiques doivent être mises en place. Les mesures prises doivent être validées par le RSSI si elles ne sont pas physiques.
RES-INTERNET-SPECIFIQUE	Cas particulier des accès spécifiques dans une entité
	Les accès spécifiques à Internet nécessitant des droits particuliers pour un usage professionnel ne peuvent être mis en place que sur dérogation dûment justifiée et depuis des machines situées dans un sous-réseau spécifique, après validation préalable du RSSI.
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.
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.

VIII. Architecture des systèmes d'information

ARCHI-HEBERG	Principes d'architecture de la zone d'hébergement
	D'une manière générale, l'architecture des infrastructures des centres informatiques est conçue de façon à satisfaire l'ensemble des besoins en disponibilité, confidentialité, traçabilité et intégrité. Le principe de défense en profondeur doit être respecté, en particulier par la mise en œuvre successive de « zones démilitarisées » (DMZ), d'environnements de sécurité en zone d'hébergement, de machines virtuelles ou physiques dédiées, de réseaux locaux virtuels (VLAN) appropriés, d'un filtrage strict des flux applicatifs et d'administration.
ARCHI-STOCKCI	Architecture de stockage et de sauvegarde
	Le réseau de stockage et de sauvegarde pour les besoins des centres informatiques repose sur une architecture consacrée.

IX. Exploitation des systèmes d'information

EXP-SAUV	Politique de sauvegarde
	Une politique de sauvegarde des éléments critiques doit être formalisée et mise en œuvre.
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 par la DSI. Les traces doivent être accessibles au correspondant local de la SSI 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-DOC-CONFIG	**Documentation des configurations**
	La configuration standard des ressources informatiques doit être documentée et mise à jour à chaque changement notable.
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-DROITS	**Droits d'accès aux ressources**
	Après avoir déterminé le niveau de sensibilité, le besoin de diffusion et de partage des ressources, les droits d'accès aux ressources doivent être gérés suivant les principes suivants : besoin d'en connaître (chaque utilisateur n'est autorisé à accéder qu'aux ressources pour lesquelles on lui accorde explicitement le bénéfice de l'accès) et moindre privilège (chaque utilisateur accède aux ressources avec le minimum de privilèges lui permettant de conduire les actions explicitement autorisées pour lui).
EXP-PROC-AUTH	**Autorisations d'accès des utilisateurs**
	Toute action d'autorisation d'accès d'un utilisateur à une ressource des SI, qu'elle soit locale ou nationale, 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-CERTIFS	**Utilisation de certificats électroniques**
	Les règles du référentiel général de sécurité pour les certificats électroniques sont appliquées si possible, en fonction des possibilités offertes par le ministère de tutelle.
EXP-QUAL-PASS	**Contrôle systématique de la qualité des mots de passe**
	Des moyens techniques permettant d'imposer la politique de mots de passe, par exemple pour s'assurer du respect de l'éventuelle obligation relative à l'usage de caractères spéciaux, doivent être mis en place.
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-RESTR-DROITS	**Restriction des droits**
	Sauf exception dûment motivée et validée par le RSSI, les utilisateurs n'ont pas de droits d'administration.
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 doivent être tracées de manière à pouvoir imputer individuellement les actions d'administration.
EXP-CENTRAL	**Centraliser la gestion du système d'information**
	Afin de gérer efficacement un grand nombre de postes d'utilisateurs, de serveurs ou d'équipements en réseau, les administrateurs doivent utiliser des outils centralisés, permettant l'automatisation de traitements quotidiens et offrant une vue globale et pertinente sur le système d'information.
EXP-SECX-DIST	**Sécurisation des outils de prise de main à distance**
	La prise de main à distance d'une ressource informatique locale ne doit être réalisable que par les agents autorisés par l'équipe locale chargée des SI, sur les ressources informatiques de leur périmètre.
EXP-DOM-POL	**Définir une politique de gestion des comptes du domaine**
	Une politique explicite de gestion des comptes du domaine doit être établie.
EXP-DOM-PASS	**Configurer la stratégie des mots de passe des domaines**
	La politique de gestion des mots de passe doit être conçue de façon à protéger contre les attaques par essais successifs de mots de passe. Une complexité minimale dans le choix des mots de passe doit être imposée aux utilisateurs.
EXP-DOM-NOMENCLAT	**Définir et appliquer une nomenclature des comptes du domaine**
	La gestion des comptes doit s'appuyer sur une nomenclature adaptée, afin de pouvoir distinguer selon leur usage les comptes d'utilisateur standard, les comptes d'administration (domaine, serveurs, postes de travail) et les comptes de service.
EXP-DOM-RESTADMIN	**Restreindre au maximum l'appartenance aux groupes d'administration du domaine**
	L'appartenance aux groupes du domaine ADMINISTRATEURS DE L'ENTREPRISE et ADMINISTRATEURS DU DOMAINE n'est nécessaire que dans de très rares cas. Les opérations les plus courantes doivent être effectuées avec des comptes du domaine membres des groupes locaux d'administration des ordinateurs ou ayant une délégation d'administration.

EXP-DOM-OBSOLET	**Désactiver les comptes du domaine obsolètes**
	Il est nécessaire de désactiver dans les meilleurs délais, voire de supprimer, les comptes obsolètes, que ce soient des comptes d'utilisateur (administrateur, service ou utilisateur standard) ou des comptes de machine.
EXP-DOM-ADMINLOC	**Améliorer la gestion des comptes d'administrateur locaux**
	Afin d'empêcher la réutilisation des empreintes d'un compte d'utilisateur local d'une machine à une autre, il faut soit utiliser des mots de passe différents pour les comptes locaux d'administration, soit interdire la connexion à distance via ces comptes.
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 validés par le RSSI.
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.
EXP-JOUR-SUR	**Journalisation des alertes**
	Chaque système doit disposer de dispositifs de « journalisation » permettant de conserver une trace des événements de sécurité.
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'équipe en charge de la SSI doit procéder, 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-MAIT-MAT	Maîtrise des matériels
	Les postes de travail, y compris dans le cas d'une location, sont fournis à l'utilisateur par l'entité, gérés et configurés sous la responsabilité de l'entité. La connexion d'équipements non maîtrisés, non administrés ou non mis à jour par l'entité, qu'il s'agisse d'ordiphones, d'équipements informatiques nomades et fixes ou de supports de stockage amovibles, sur des équipements et des réseaux professionnels est par défaut interdite. Elle peut être autorisée après accord du RSSI, qui définira les conditions de sécurité à mettre en œuvre.
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-REAFFECT	Réaffectation de matériels informatiques
	Une procédure de gestion des postes et des supports dans le cadre de départs de personnel ou de réaffectations à de nouveaux utilisateurs doit être mise en place et validée par le RSSI. Elle doit définir les conditions de recours à un effacement des données.
EXP-ACC-DIST	Accès à distance au système d'information de l'organisme
	Les accès à distance aux SI de l'entité (accès dits « nomades ») doivent être réalisés via des réseaux privés virtuels (VPN) de confiance.
EXP-IMP-SENS	Impression des informations sensibles
	Les impressions d'informations sensibles doivent être effectuées selon une procédure garantissant un contrôle par l'utilisateur, du déclenchement de l'impression jusqu'à la récupération du support imprimé.
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-LTP	Logiciels en tiers présentation
	La mise en œuvre d'une configuration renforcée est obligatoire sur les logiciels déployés pour le tiers présentation (exemples: serveur Web, Reverse Proxy).

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-ADMIN	Flux d' administration
	Les opérations d'administration sur les ressources locales d'une entité doivent s'appuyer sur des protocoles sécurisés. D'une manière générale, il convient de différencier deux types de flux d'administration : les flux d'administration de l'infrastructure, réservés aux agents du centre informatique, et les flux d'administration des applications métier, réservés à la direction métier. L'attribution des droits d'administration doit respecter cette différenciation. Les deux types de flux d'administration doivent être dans la mesure du possible cloisonnés.
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).

X. Sécurité du poste de travail

PDT-REAFFECT	Réaffectation du poste de travail
	Les données professionnelles contenues sur un poste de travail réaffecté qui doivent être transférées au nouveau bénéficiaire du poste sont définies en accord avec le responsable hiérarchique métier.
PDT-PRIVIL	Privilèges des utilisateurs sur les postes de travail
	La gestion des privilèges des utilisateurs sur leurs postes de travail doit suivre le principe du moindre privilège. Chaque utilisateur ne doit ainsi disposer que des privilèges nécessaires à la conduite des actions relevant de sa mission.
PDT-ADM-PRIV	Utilisation des privilèges d'accès des administrateurs
	Les privilèges d'accès des administrateurs doivent être utilisés uniquement pour les actions d'administration le nécessitant.
PDT-ADM-LOCAL	Gestion du compte de l'administrateur local
	L'accès au compte de l'administrateur local sur les postes de travail doit être strictement limité aux équipes en charge de l'exploitation et du support sur ces postes de travail.
PDT-STOCK	Stockage des informations
	Dans la mesure du possible, les données traitées par les utilisateurs doivent être stockées sur des espaces en réseau, eux-mêmes sauvegardés selon les exigences des entités et en accord avec les règles de sécurité en vigueur.
PDT-SAUV-LOC	Sauvegarde et synchronisation des données locales
	Dans le cas où des données doivent être stockées localement sur le poste de travail, des moyens de synchronisation ou de sauvegarde doivent être fournis aux utilisateurs.
PDT-PART-FIC	Partage de fichiers
	Le partage de répertoires ou de données hébergées localement sur les postes de travail n'est pas autorisé.
PDT-SUPPR-PART	Suppression des données sur les postes partagés
	Les données présentes sur les postes partagés (portable de prêt, par exemple) doivent être supprimées entre deux utilisations, dès lors que les utilisateurs ne disposent pas du même besoin d'en connaître.

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 ou le ministère de tutelle.
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. Sécurité du développement des systèmes

DEV-FUITES	Limiter les fuites d'information

Les fuites d'informations techniques sur les logiciels utilisés permettent aux attaquants de déceler plus facilement d'éventuelles vulnérabilités.

DEV-LOG-ADHER	Réduire l'adhérence des applications à des produits ou technologies spécifiques

Le fonctionnement d'une application s'appuie sur un environnement logiciel et matériel. En phases de conception et de spécification technique, il est nécessaire de s'assurer que les applications n'ont pas une trop forte adhérence vis-à-vis des environnements sur lesquels elles reposent. En effet, l'apparition de failles sur un environnement a de fait un impact sur la sécurité des applications qui en dépendent. En plus du maintien en condition de sécurité propre à l'application, il est donc nécessaire de pouvoir faire évoluer son environnement pour garantir sa sécurité dans la durée.

DEV-LOG-CYCLE	Intégrer la sécurité dans le cycle de vie du logiciel

La sécurité doit être intégrée à toutes les étapes du projet, depuis l'expression des besoins jusqu'à la maintenance applicative, en passant par la rédaction du cahier des charges et les phases de recette.

DEV-LOG-WEB	Améliorer la prise en compte de la sécurité dans les développements Web

Les développements Web, en particulier les développements en PHP, font l'objet de problèmes de sécurité récurrents qui ont conduit à la constitution de référentiels de sécurité.
Ces référentiels ont pour objectif de fixer des règles de bonne pratique à l'usage des développeurs.
Ce sont des règles d'ordre générique ou pouvant être spécifiques à un langage (PHP, ASP, .NET, etc.).

DEV-LOG-AUD	Audit des développements Web

Avant mise en production, les développements Web doivent faire l'objet d'audits de code par l'outil proposé par la DNE.
Des audits réguliers doivent être effectués.

DEV-LOG-PASS	Calculer les empreintes de mots de passe de manière sécurisée

Lorsqu'une application doit stocker les mots de passe de ses utilisateurs, il est important de mettre en œuvre des mesures permettant de se prémunir contre les attaques documentées : attaques par dictionnaire, attaques par tables dites « arc-en-ciel », attaques par force brute, etc.