Aix*Marseille université
Socialement engagée

CONSEIL D'ADMINISTRATION D'AIX-MARSEILLE UNIVERSITE

DELIBERATION n° 2021/09/21-07-CA

Le **Conseil d'administration**, en sa séance du 21 septembre 2021, sous la présidence d'Éric BERTON, Président,

Vu le Code de l'Education,
Vu les Statuts d'Aix-Marseille Université modifiés,

Considérant que l'Université d'Aix-Marseille doit se doter d'une Politique de Sécurité des systèmes Informatiques (PSSI) ;

Considérant que les points importants de cette PSSI et les priorités qui en découle pour l'année à venir portent, notamment, sur :

- Sécurité physique des locaux
- Sécurité des donnés
- Authentification pour l'envoi des mails, gestion des redirections
- Sauvegarde hors ligne
- Gestion des droits d'accès aux ressources informatiques d'AMU
- Sensibilisation / formation des personnels
- Journalisation, gestion, exploitation des journaux de connexion et d'actions

DECIDE :

OBJET : Présentation de la Politique de Sécurité des Systèmes Informatiques (PSSI) et des objectifs pour l'année à venir

Le Conseil d'administration approuve la Politique de Sécurité des Systèmes Informatiques (PSSI) et les objectifs pour l'année à venir, tels qu'annexés à la présente délibération.

Cette délibération est adoptée à l'unanimité des membres présents et représentés.

Membres en exercice : 36
Quorum : 18
Présents et représentés : 28

Fait à Marseille le 21 septembre 2021,

Eric BERTON,
Président d'Aix-Marseille Université

Université d'Aix Marseille AMU

ANNEXE A LA DELIBERATION N°2021/09/21-07-CA
Séance du Conseil d'administration du 21 septembre 2021

Proposition de

Politique de Sécurité des Systèmes d'Information (PSSI) pour AMU

conforme à la

Politique de Sécurité des Systèmes d'Information de l'Etat (PSSIE)

Version 3.9

20/01/2020

René ARON, RSSI

Table des matières

I - Préambule

Ce document présente une proposition de politique de sécurité des systèmes d'information (PSSI) pour l'université d'Aix-Marseille, en conformité avec les objectifs de sécurité, définis dans les documents de Politique de Sécurité des Systèmes d'Information de l'Etat (PSSIE), ainsi qu'avec l'ensemble des textes afférents.

Cet ensemble de directives prend également en compte les connaissances des besoins de sécurité acquises en milieu universitaire, et plus particulièrement liées à l'université d'Aix-Marseille.

Afin de couvrir au mieux les risques liés aux systèmes d'information de l'établissement, une analyse de risques a été effectuée, ce qui a permis d'adapter encore un peu plus les directives de sécurité proposées.

II - Situation et modalités d'application de la Sécurité des Systèmes d'Information

A - Situation

L'Université d'Aix-Marseille accueille actuellement 80000 étudiants et 8000 personnels. Les 52 sites géographiques de l'Université sont interconnectés via un réseau régional haut débit, lui-même raccordé au Réseau National de télécommunications pour la Technologie l'Enseignement et la Recherche (Renater).

B - Champ d'application de la SSI

La politique de sécurité des systèmes d'information (PSSI) de l'Université s'applique à l'ensemble des systèmes d'information présents dans les différentes entités de l'établissement.

Cela recouvre :

- le système informatique de gestion,
- les systèmes et applications de communication (messagerie, sites web…),
- les systèmes de stockage des données,
- les systèmes de sauvegarde
- les applications spécifiques des composantes de l'établissement (traitements de données …),
- les systèmes reposant sur les ressources informatiques (contrôle d'accès, vidéosurveillance, visioconférence, ToIP/VoIP …),
- les réseaux de connexions avec les partenaires et cotutelles d'entités de recherche (CNRS, INSERM…).

C - Critères de sécurité

La sécurité du Système d'Information repose sur les critères suivants :

- **Confidentialité** : « La confidentialité est la propriété qu'une information n'est ni disponible ni divulguée aux personnes, composantes ou processus non autorisés » norme ISO 7498-2 (ISO90).
- **Intégrité** : « L'intégrité est la prévention d'une modification non autorisée de l'information » norme ISO 7498-2 (ISO90).
- **Disponibilité** : Faculté de pouvoir accéder aux données au moment nécessaire par les utilisateurs autorisés.
- **Traçabilité** : Faculté de pouvoir indiquer quelle action a été réalisée par quel processus ou utilisateur, à quelle date, à partir de quel ordinateur ou accès système et/ou réseau.

Ces critères de sécurité sont applicables :

- aux moyens techniques mis en œuvre dans le système d'information (serveurs, ordinateurs des postes de travail, matériels réseaux),
- aux applications,
- aux données traitées.

Les données doivent être référencées selon un système de classification (gestion, nominative, scientifique, stratégique, défense…) pour déterminer le degré de protection qui devra leur être appliqué.

D - Risques

L'identification des risques auxquels l'établissement peut être confronté est l'étape nécessaire afin d'évaluer quels sont les types de menaces à prévenir et les moyens à mettre en œuvre afin d'y faire face.

La méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité – ANSSI) permet cette identification et le classement des risques dans les catégories suivantes :

- les accidents : sinistres naturels, altération accidentelle des données, altération accidentelle des ressources…
- les attaques visant les ressources informatiques : altération des données, vol ou détournement de ressources, virus et programmes informatiques pirates…
- les attaques visant directement le système d'information : modification et/ou vol de données, vol de supports de données, attaques fonctionnelles de serveurs (déni de service…)…

Pour chaque risque identifié, la probabilité de réalisation doit être évaluée, ainsi que les facteurs favorisant sa survenue (manque d'information du personnel, respect non strict des consignes de sécurité…).

E - Chaîne de responsabilités de la SSI au sein de l'université

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), émet des directives et recommandations au niveau national. Celles-ci sont transmises pour mise en œuvre, par le Haut Fonctionnaire de Défense et de Sécurité (HFDS) et son Adjoint en charge du ministère de l'éducation nationale, de l'enseignement supérieur et de la recherche, ainsi que par le Fonctionnaire de Sécurité des Systèmes d'Information (FSSI) de ce même ministère, qui travaille avec le HFDS Adjoint.

La Politique de Sécurité des Systèmes d'Information de l'Université d'Aix-Marseille s'inscrit dans ce cadre.

La responsabilité de la sécurité des systèmes d'information de l'Université d'Aix-Marseille, relève en premier lieu du Président de l'université en tant qu'Autorité Qualifiée pour la Sécurité des Systèmes d'Information (AQSSI).

Dans cette fonction de sécurité, le Président est assisté par le Responsable de la Sécurité des Systèmes d'Information (RSSI), ainsi que par le Fonctionnaire de Sécurité Défense (FSD).

La gestion normale de la Sécurité des Systèmes d'Information relève de la responsabilité du RSSI et de ses adjoints, s'appuyant sur :

- la chaîne fonctionnelle de la SSI, constituée de Correspondants Sécurité Système d'Information (CSSI) dans les différentes structures de l'établissement, pour la diffusion d'information de sécurité, la remontée d'information de sécurité, la sensibilisation, l'application des règles, le respect des chartes…
- la chaîne opérationnelle de la SSI, constituée par les personnels techniques travaillant à la définition et la mise en œuvre des recommandations de sécurité relatives à l'accès aux locaux, l'administration des systèmes, du réseau, des services, des applications métiers.
- la chaîne d'alerte de la SSI chargée d'assister le RSSI en cas d'incident de sécurité majeur.

Les responsables hiérarchiques (chefs de services, directeurs, doyens…) des entités de travail (services, laboratoires, écoles, instituts…) de l'université, sont responsables de la sécurité des systèmes d'information de leur entité, pour laquelle ils nomment un Correspondant SSI (CSSI), qui fait partie d'une ou plusieurs chaînes de la SSI évoquées ci-dessus.

Dans le cas de plusieurs entités regroupées au sein d'un pôle de compétences (groupement de laboratoires…), il est possible de nommer un seul CSSI pour une partie ou pour l'ensemble de ces entités.

Cette nomination doit être validée par l'ensemble des responsables hiérarchiques des entités pour lesquelles ce CSSI devra travailler. Les entités n'ayant pas validé le CSSI de leur pôle de compétence, devront être dotées d'un CSSI qui leur sera propre.

Les CSSI reçoivent des instructions, directives et recommandations du RSSI, et sont tenus de les mettre en œuvre. Ils doivent également appliquer et faire respecter la PSSI de l'établissement. Ils ont obligation d'informer le RSSI des incidents rencontrés dans leurs fonctions SSI.

Lorsque les entités de travail (unités de recherches…) ont plusieurs tutelles (université, CNRS…), leurs responsables hiérarchiques et leurs CSSI doivent :

- en cas d'existence d'un contrat régissant leurs tutelles, appliquer les instructions SSI prévues,
- en cas d'absence d'un contrat régissant leur tutelle, ou en cas d'absence des dispositions SSI dans le contrat régissant leurs tutelles, appliquer :
    - la PSSI de l'université
    - les dispositions SSI des autres organismes de tutelles.

Dans ce cas, les contraintes SSI les plus fortes seront celles appliquées.

Les responsables hiérarchiques de ces entités de travail ayant plusieurs tutelles, et leur CSSI, ont obligation, en cas d'incidents rencontrés dans leurs fonctions SSI, d'informer :

- le RSSI de l'université d'Aix-Marseille,
- les autres tutelles.

Une concertation pourra ainsi avoir lieu entre les différentes tutelles afin d'évoquer les suites à donner en fonction des incidents SSI rencontrés.

III - Référentiel documentaire SSI

La sécurité des systèmes d'information de l'établissement s'appuie sur un référentiel documentaire, comportant :

- Les lettres de mission du RSSI, du FSD notamment,
- Les chartes :
- « charte régissant l'usage du système d'information de l'université d'Aix-Marseille » (qui s'applique àtous les utilisateurs : étudiants, personnels, hébergés, etc.),
- chartes informatiques des partenaires de cotutelle d'entités de travail,
- chartes d'utilisation de réseaux informatiques (RENATER…),
- La politique de sécurité des systèmes d'information (PSSI),
- Le plan de continuité d'activité (PCA),
- Le plan de reprise d'activité (PRA),
- - Les textes relatifs aux structures et à la sensibilité des données

  Instruction générale interministérielle sur la protection du secret n°2092/DN/SIG du 19 mai 1952,

  Instruction générale interministérielle n°1300 (de 2011)

- Les fichiers de gestion des traces d'actions dans les systèmes d'information…

IV - Structures et responsabilités

A partir du référentiel documentaire, l'établissement met en place une structure fonctionnelle SSI.

A - Accès aux systèmes d'information et aux ressources informatiques

Un utilisateur (étudiant, personnel titulaire ou contractuel, hébergé…) des systèmes d'information et de ressources informatiques doit être informé dès son arrivée, des conditions d'utilisation. Son arrivée, ses changements de responsabilités et fonctions, ainsi que son départ doivent être suivis par l'administration, afin de gérer ses droits d'accès aux ressources informatiques de l'établissement. Cet accès doit être contrôlé (identification, authentification) et adapté aux besoins de l'utilisateur (profil utilisateur, droits d'accès…), en fonction de ses responsabilités et de ses droits juridiques.

B - Information des acteurs SSI sur leurs droits et devoirs

Les acteurs SSI doivent être informés de leurs droits et devoirs dans ce domaine. Dans l'exercice de leurs fonctions SSI, ils sont tenus à leur devoir de réserve, ainsi qu'éventuellement au secret professionnel.

C - Responsable de la Sécurité des Systèmes d'Information

Le Responsable de la Sécurité des Systèmes d'Information (RSSI) est nommé par le Président de l'Université d'Aix-Marseille (AQSSI : Autorité Qualifiée de Sécurité des Systèmes d'Information de l'établissement), qui lui attribue une lettre de missions.

Le RSSI exerce sous l'autorité directe du Président de l'Université d'Aix-Marseille, notamment les activités suivantes (la lettre de missions contient le détail de ces activités):

- Contribuer activement à l'élaboration d'une politique de sécurité des systèmes d'information et la mettre en œuvre,
- Gérer les dossiers internes et externes relevant de la sécurité des systèmes d'information,
- Viser tous les projets de l'établissement, en lien avec son domaine de compétences, afin de veiller à la mise en oeuvre des éléments technologiques nécessaires à l'application de la PSSI dans chacun d'eux,
- Coordonner, animer le réseau des correspondants sécurité de l'établissement,
- Exploiter et relayer les informations relatives à la sécurité des systèmes d'information en provenance des organismes et structures d'alertes (CERTA, du CERT-Renater, ANSSI, HFDS…) avec lesquels il est en contact,
- Faire connaître et respecter la charte déontologique Renater ainsi que la charte d'utilisation des moyens informatiques et réseau de l'établissement,
- Proposer et mettre en œuvre des actions de sensibilisation et d'information de tous les utilisateurs aux aspects sécurité des systèmes d'information,
- Être l'intermédiaire direct en cas de problème entre le Président de l'université et les autorités compétentes.

D - Surveillance informatique

Dans le cadre de l'application d'une politique de sécurité des systèmes d'information, il est nécessaire de pouvoir surveiller les flux de données sur le réseau et de tracer les actions effectuées. Les dispositifs de surveillance mis en œuvre doivent respecter la réglementation en vigueur ainsi que les principes de proportionnalité (la nature et le dimensionnement des moyens techniques utilisés doivent être adaptés à l'objectif de sécurité visé) et de transparence (information des utilisateurs sur les moyens techniques mis en œuvre pour la SSI).

V - Sécurité physique

A - Sécurité physique des locaux abritant les SI.

Objectif fixé dans la PSSIE : inscrire la sécurisation physique des SI dans la sécurisation physique des locaux et dans les processus associés.

1 - Découpage des sites en zones de sécurité

La PSSIE prévoit qu'un « *découpage des sites en zones physiques de sécurité doit être effectué, en liaison avec le RSSI, les correspondants SSI et les services en charge :*

- *de l'immobilier,*
- *de la sécurité physique,*
- *des moyens généraux.*

Pour chaque zone de sécurité, des critères précis d'autorisation d'accès sont établis. »

Dans la situation actuelle, cela s'applique aux ZRR ou aux laboratoires devant devenir des ZRR.

2 - Accès réseau en zone d'accueil du public

Les accès réseau destinés au public reçu par l'établissement doivent être filtrés / isolés du reste du réseau informatique de l'université.

3 - Protection des informations sensibles au sein des zones d'accueil du public.

De façon générale, le traitement d'informations sensibles au sein des zones d'accueil du public doit être évité.

Cependant, lorsque cela s'avère nécessaire pour certains services, afin d'accomplir leurs missions, (ex. Scolarité/inscriptions), des mesures particulières sont alors adoptées en regard de l'état de l'art, notamment en matière de protection audiovisuelle, ainsi qu'en matière de protection des informations stockées sur les supports de données (ex. disques durs des ordinateurs utilisés pour ces missions).

4 - Sécurité physique des locaux techniques

L'accès aux locaux techniques abritant des équipements d'alimentation et de distribution d'énergie, des équipements de serveurs ou des équipements de réseau et de téléphonie, doit être physiquement protégé.

Ce contrôle d'accès doit être effectué par du badgeage, par un digicode ou à défaut la tenue d'un registre des entrées/sorties.

5 - Protection des câbles électriques et de télécommunications

Le câblage réseau doit être protégé contre les dommages et les interceptions des communications qu'ils transmettent.

De ce fait, les panneaux de raccordements et les zones de distribution du réseau doivent être placés idéalement, en dehors des zones d'accueil du public et leur accès doit être contrôlé.

6 - Contrôles anti-piégeages

Sur les systèmes d'information particulièrement sensibles, des contrôles « anti-piégeages » (antiespionnage) réguliers, seront effectués par du personnel formé. Conformément à la PSSIE, un appel à des services spécialisés (opérations dites de « dépoussiérage ») est réalisable.

B - Sécurité physique des services informatiques.

1 - Découpage des locaux en zones de sécurité

L'accès aux locaux des services informatiques (répartis en différentes zones, ex : salle machines...) doit être sécurisé, en liaison avec le RSSI et les services en charge de l'immobilier, de la sécurité physique et des moyens généraux. Ce contrôle d'accès doit être effectué par du badgeage, par un digicode ou à défaut la tenue d'un registre des entrées/sorties.

2 - Convention de service en cas d'hébergement tiers

Dans le cas où un tiers gère tout ou partie des locaux des services informatiques, une convention de service, définissant les responsabilités mutuelles en matière de sécurité, doit être établie entre ce tiers et l'entité ou le ministère.

3 - Contrôle d'accès physique

L'accès aux zones internes des services informatiques (zones autorisées uniquement au personnel des services informatiques ou aux visiteurs accompagnés) et restreintes (zones autorisées aux seules personnes habilitées ou aux visiteurs accompagnés) doit reposer sur un dispositif de contrôle d'accès physique (ex. carte à puce professionnelle).

Ce dispositif doit s'appuyer sur des produits qualifiés, lorsqu'ils sont disponibles, et bénéficier d'un maintien en condition de sécurité rigoureux.

Cela concerne, notamment, l'accès aux bureaux du personnels du service informatique de l'établissement.

4 - Délivrance des moyens d'accès physique

La délivrance et la restitution des moyens d'accès physique (ex. carte à puce professionnelle) doivent respecter un processus formel permettant de s'assurer de l'identité de la personne, s'appuyant sur le processus d'arrivée et de départ du personnel, géré par la direction des ressources humaines de l'établissement.

Le personnel autre que celui explicitement autorisé et habilité, mais néanmoins appelé à intervenir dans les zones sensibles (entretien ou réparation des bâtiments, des équipements non informatiques, nettoyage, visiteurs, ...), intervient systématiquement et impérativement sous surveillance permanente.

5 - Traçabilité des accès

Dans les ZRR, une traçabilité des accès, par les visiteurs externes, aux zones restreintes doit être mise en place. Ces traces sont alors conservées un an sur un registre des entrées/sorties, dans le respect des textes protégeant les données personnelles.

6 - Local énergie

L'alimentation secteur des équipements doit être conforme aux règles de l'art, de façon à se prémunir des atteintes à la sécurité des personnes et des équipements liées à un défaut électrique.

Les salles machines sont dotées d'onduleurs et de groupes électrogènes.

7 - Climatisation

Un dispositif de climatisation dimensionné en fonction des besoins énergétiques des systèmes informatiques doit être installé dans les salles machines. Des procédures de réaction en cas de panne, connues du personnel, sont élaborées et vérifiées annuellement. Ces dispositions visent à prévenir toute surchauffe des équipements, pouvant engendrer une perte des services voire une détérioration du matériel.

Des délais d'intervention doivent être imposés dans les contrats de maintenance pour les équipements de climatisation dans le data center, afin de garantir le niveau de disponibilité nécessaire aux données hébergées.

8 - Lutte contre l'incendie

Les salles machines sont dotées de dispositifs contre l'incendie. L'installation de ces matériels de protection contre le feu est obligatoire, conformément à la PSSIE. Des procédures de réaction à un incendie sont définies et régulièrement testées. Les salles techniques doivent être propres. Aucun carton, papier, ou autre source potentielle de départ de feu ne doit être entreposé dans ces locaux.

9 - Lutte contre les voies d'eau

Une étude sur les risques dus aux voies d'eau, impactant les services informatiques et notamment les locaux techniques (salles machines, locaux réseaux...) doit être réalisée. Cette étude doit notamment prendre en compte le risque de fuite sur un collecteur d'eau douce.

C - Sécurité du Système d'Information de sûreté.

1 - Définition du SI de sûreté.

Le système d'information de sûreté est constitué par l'ensemble des dispositifs informatiques déployés sur les sites géographiques de l'établissement et qui concourent à sa sécurisation.

2 - Sécurisation du SI de sûreté.

Des mesures de protection physiques adaptées aux spécificités physiques et géographiques des lieux où sont situés les systèmes d'information doivent être définies et appliquées (ex. contrôle d'accès par carte à puce professionnelle).

Pour ce faire, une analyse de risques conduit à la désignation des « briques essentielles » dont il faut assurer la protection contre des actes malveillants.

En outre, les données provenant des systèmes de vidéosurveillance et des systèmes visiophones devront transiter sur des Vlans dédiés.

Un système de gestion de la sécurité du système d'information de sûreté (s'inspirant de la norme ISO 27001) assure le maintien en condition de sécurité. L'emploi de produits labellisés, quand ils existent, est fortement recommandé.

D - Architecture sécurisée des centres informatiques.

1 - Principes d'architecture de la zone d'hébergement

L'architecture des infrastructures des services informatiques est conçue de façon à satisfaire l'ensemble des besoins en disponibilité, confidentialité, traçabilité et intégrité.

Cette architecture doit prévoir, par exemple, la redondance des serveurs hébergeant des services critiques ou des données classifiées sensibles.

Le principe de défense en profondeur doit être respecté, notamment 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.

2 - Architecture de stockage et de sauvegarde

Le réseau de stockage/sauvegarde pour les besoins des services informatiques repose sur des réseaux logiques dédiés (VLAN) à cet effet. Ils sont gérés campus par campus.

3 - Passerelle Internet

Les interconnexions Internet passent obligatoirement par les passerelles nationales homologuées (ex. RENATER).

VI - Sécurité des données

A - Disponibilité, intégrité, confidentialité et traçabilité des données et actions de sauvegarde

Les quatre critères de sécurité des données (disponibilité, intégrité, confidentialité et traçabilité) conduisent à la mise en place de processus de traitement dont l'objectif est la prévention de la mauvaise utilisation, de la modification indue ou encore de la perte de ces données et de leur divulgation.

Ainsi, ces processus relatifs aux données, concernent :

- les accès,
- les traitements,
- le stockage,
- les flux d'échange entre systèmes d'informations,
- les accès aux applications et services numériques informatiques.

B - Sauvegardes

La sécurité des données repose également sur :

- des processus de sauvegarde des données avec une périodicité déterminée en fonction de leur nature,
- des processus de restauration éprouvés.

Les sauvegardes de données :

- doivent reposer sur des processus garantissant leur confidentialité et leur intégrité,
- ne doivent pas être soumises aux mêmes risques de sinistres que les données sauvegardées, notamment, en stockant les sauvegardes dans un lieu éloigné des sites de production.

Plusieurs types de sauvegardes seront mis en œuvre :

- des sauvegardes de production (restauration des données d'exploitation),
- des sauvegardes de reprise d'activités complètes (permettant un remontage complet des systèmes d'information sur d'autres machines, voire en externe à l'établissement),
- des sauvegardes de données d'utilisation des systèmes d'information (permettant de justifier sur requête judiciaire).

La périodicité, la durée de conservation et les moyens techniques de sauvegarde seront déterminés par une étude de la nature des données, en regard des dispositions réglementaires et légales en vigueur.

C - Données à caractère personnel

Les données à caractère personnel sont à classer dans la catégorie des données sensibles.

Les bases de données susceptibles de contenir des données à caractère personnel (au sens de la loi n°78-17 du 6 janvier 1978 modifiée, relative à l'informatique, aux fichiers et aux libertés), ainsi que les traitements

afférents, doivent faire l'objet de formalités de déclarations et/ou demandes requises, par le Correspondant Informatique et Libertés (CIL) et/ou Responsable de la protection des données (DPO) de l'université, auprès de la CNIL.

D - Sécurité des données sensibles

1 - Données classifiées

Dans le cas général, il est formellement interdit de stocker et de transmettre des données classifiées défense, sauf disposition particulière et explicite permettant ces actions, via la mise en œuvre de moyens techniques particuliers et agréés au niveau national.

Il est à noter que « l'habilitation secret défense n'est pas suffisante pour accéder à un document classifié ». En effet, il est également nécessaire que : « le besoin d'en connaître », c'est-à-dire la nécessité de prendre connaissance du document dans l'exercice de ses fonctions, soit justifié (cf. http://www.pleiade.education.fr/ - Communauté HFDS - Protection du secret et habilitation).

De plus, pour certains sujets traités par les doctorants et classifiés « confidentiel » ou « secret défense », un contrôle strict doit être dispensé par la Direction Générale de l'Armement (DGA).

2 - Données non classifiées

Afin d'assurer la sécurité des données, il est également nécessaire d'identifier les données non classifiées qui présentent un caractère sensible.

Ce processus d'identification doit être itératif avec une périodicité déterminée.

Un contrôle d'accès (authentification, contrôle d'autorisation), de traitement, de stockage et/ou d'échange (par chiffrement) sera mis en place pour assurer la sécurité de ces données particulières.

3 - Supports physiques de données sensibles

Avant la sortie d'inventaire de matériels supports de données sensibles, en vue d'une sortie physique de ces matériels hors des locaux sécurisés de l'université, il doit être procédé à un effacement utilisant une méthode validée par les services de l'Etat, en charge de la SSI. En cas d'impossibilité d'effacement, les supports matériels devront être détruits de façon complète et ne permettant pas une reconstruction physique de ces supports.

E - Chiffrement

Les données sensibles doivent faire l'objet d'un chiffrement pour leur stockage et pour les échanges afférents. Les matériels et logiciels utilisés pour gérer ces données sensibles doivent avoir reçu l'agrément de l'ANSSI.

Afin de pouvoir restituer les données en clair, il est nécessaire de stocker dans un lieu sécurisé (distinct du lieu de stockage des données sensibles), une copie des clés permettant le déchiffrement.

VII - Gestion des biens

A - Cartographie des systèmes d'information

1 - 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 disposition du RSSI, ainsi que 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.

2 - Cartographie

La cartographie indique :

- les salles informatiques :
  - par des schémas logiques et fonctionnels,
  - par des schémas montrant les implantations physiques des matériels.
- les architectures des réseaux :
  - par des schémas logiques et fonctionnels, présentant les matériels notamment actifs etles points névralgiques...,
  - par des schémas montrant les implantations physiques des matériels.
- les applications
- le niveau de sécurité attendu.

Cette cartographie est maintenue à jour et tenue à disposition du RSSI, ainsi que du FSSI et de l'ANSSI en cas de besoin de coordination opérationnelle.

B - Qualification et protection de l'information.

1 - Qualification des informations.

Les documents administratifs sensibles (au sens de « classifiés ») sont actuellement cantonnés dans des structures de la Présidence ou proche de celles-ci. Ces documents arrivent généralement, déjà pourvus du marquage adéquat, depuis les instances ministérielles. Lorsqu'ils proviennent d'autres structures de l'Etat (ex. Préfecture, Gendarmerie), leur marquage peut être à effectuer.

Les documents liés à la Recherche, émis par les laboratoires, relèvent de ces structures pour leur marquage.

2 - 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.

Ainsi, les bureaux sont pourvus de dispositifs de destruction de papier, afin d'éviter les pertes d'informations. Les utilisateurs sont informés, dans leurs structures de travail, du besoin de destruction des documents imprimés devenus inutiles.

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

---

A - Risques.

1 - Homologation de sécurité des systèmes d'information : une obligation.

Tout système d'information doit faire l'objet d'une décision d'homologation de sa sécurité avant sa mise en exploitation dans les conditions d'emploi définies. L'homologation est l'acte selon lequel l'autorité atteste formellement auprès des utilisateurs que le système d'information est protégé conformément aux objectifs de sécurité fixés. La décision d'homologation est prise par l'autorité d'homologation (désignée par l'AQSSI), le cas échéant après avis de la commission d'homologation.

Dans le cas de l'université, les systèmes d'information sont déjà mis en œuvre. Ils pourront faire l'objet d'une homologation, *a posteriori*.

2 - Homologation de sécurité des systèmes d'information : basée sur une analyse de risques.

La décision de mettre en œuvre une homologation de sécurité des systèmes d'information de l'établissement s'appuie sur une analyse de risques adaptée aux enjeux des systèmes considérés, et précise les conditions d'emploi (analyse de risques systématique pour tous les systèmes d'information avec un niveau de profondeur adapté aux enjeux).

B - Maintien en condition de sécurité.

1 - 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 de l'autorité d'homologation, à défaut de l'AQSSI ou du RSSI, de la conception et de la spécification des systèmes d'information jusqu'à leurs retraits du service.

Plus spécifiquement à l'université, la sécurité des systèmes d'information dans les projets de développements informatiques est prise en compte directement par les chefs de ces projets. Ces projets ne constituent pas en eux-mêmes des systèmes d'information complets, mais des parties ou « briques » fonctionnelles.

Pour les ensembles logiciels ou briques logicielles acquis auprès d'éditeurs (AMUE...), la sécurité des systèmes d'information est assurée par les éditeurs, en regard de l'état de l'art et/ou des cahiers des charges établis par les autorités nationales qui ont concouru aux développements de ces ensembles logiciels.

Pour les ensembles logiciels ou briques logicielles développés par des prestataires de service, à la demande de l'université et de ses partenaires éventuels, la sécurité des systèmes d'information est assurée par ces prestataires, en regard de l'état de l'art et du cahier des charges établi par l'université et ses partenaires éventuels.

2 - Mise en œuvre au quotidien de la SSI

La sécurité des systèmes d'information de l'établissement est assurée au quotidien par la mise en œuvre des pratiques d'hygiène informatique et des mesures décrites dans la charte informatique de l'établissement.

3 - Créer un tableau de bord SSI.

Un tableau de bord SSI est mis en place et tenu à jour par l'actualisation automatique des indicateurs qui le composent. Il fournit à la Présidence de l'établissement, ainsi qu'au RSSI, une vision générale du niveau de sécurité et de son évolution. Il est utilisé pour le pilotage de la SSI de l'établissement.

Il fournit également un niveau d'informations techniques agrégées, destiné au RSSI et aux personnels du service informatique, afin de suivre la SSI au quotidien et de pouvoir réaliser des actions adaptées, selon les valeurs des différents indicateurs SSI.

Au niveau stratégique, le tableau de bord SSI permet de suivre l'application de la politique de sécurité des systèmes d'information et de disposer d'éléments propres à qualifier les ressources devant être allouées à la SSI.

Au niveau du pilotage, la mise en place de ce tableau de bord permet de contrôler la réalisation d'objectifs opérationnels, d'améliorer la qualité de service et de suivre la réalisation de certains objectifs de sécurité.

C - Produits et services qualifiés ou certifiés

1 - Acquisition de produits et services de confiance

Lorsqu'ils sont disponibles, des produits ou des services de sécurité labellisés (certifiés, qualifiés) par l'ANSSI doivent être utilisés.

2 - Acquisition de produits et services non labellisés

Lorsque des produits ou des services de sécurité sont nécessaires à l'établissement, mais qu'il n'y a pas de version labellisée (certifiée, qualifiée) par l'ANSSI, l'établissement choisira des produits ou services qui répondront aux exigences de l'état de l'art en matière de sécurité des systèmes d'information.

D - Maîtrise des prestations.

1 - Clauses de sécurité

Toute prestation dans le domaine des systèmes d'information est encadrée par des clauses de sécurité. Ces clauses spécifient les mesures de sécurité des systèmes d'information que le prestataire doit respecter dans le cadre de ses activités.

Les prestataires devront fournir pour toute prestation de service leur Plan d'Assurance Sécurité (PAS) précisant comment ils se conforment aux exigences de cybersécurité définies par l'établissement pour ce qui concerne leur organisation et leur système d'information.

2 - Suivi et contrôle des prestations fournies.

Le maintien d'un niveau de sécurité au cours du temps sera effectué par l'équipe encadrant la prestation pour :

- évaluer et vérifier la pertinence du cahier des charges en amont des projets,
- suivre les actions du sous-traitant et vérifier la conformité au cahier des charges,
- vérifier la conformité des réponses apportées par le sous-traitant en phase de recette,
- évaluer et vérifier le niveau de sécurité global obtenu en production.

3 - Analyse de risques

Toute opération d'externalisation s'appuie sur une analyse de risques préalable, afin de formaliser les objectifs de sécurité et définir des mesures adaptées.

L'ensemble des objectifs de sécurité formalisés par cette analyse, permet de définir une cible de sécurité servant de cadre au contrat établi avec le prestataire.

4 - Hébergement

L'hébergement des données sensibles de l'administration française (donc de l'université et de ses structures) sur le territoire national est obligatoire, sauf accord du HFDS, et dérogation dûment motivée et précisée dans la décision d'homologation des systèmes d'information de l'établissement.

5 - Hébergement et clauses de sécurité

Dans le cas d'une dérogation pour héberger des données de l'établissement auprès d'un prestataire de service, 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...).

IX - Exploitation des SI

A - Protection des informations sensibles.

1 - Protection des informations sensibles en confidentialité et en intégrité

Les informations sensibles doivent être chiffrées pour assurer leur confidentialité et leur intégrité.

2 - Utilisation d'un réseau homologué

L'utilisation d'un réseau homologué doit être mise en œuvre lorsque cela est possible.

B - Surveillance et configuration des ressources informatiques des systèmes d'information.

1 - Traçabilité des interventions sur les systèmes d'information

Les interventions de maintenance sur les ressources informatiques de l'établissement sont enregistrées dans un ensemble logiciel permettant de fournir leur historique. Ces enregistrements sont effectués selon un mode de type « déclaratif ».

Ces traces d'intervention doivent être accessibles pendant au moins un an.

2 - Configuration des ressources informatiques

Pour les informations « classifiées », les systèmes d'exploitation et les logiciels doivent être durcis. Les configurations et mises à jour sont appliquées dans le strict respect des guides ou procédures en vigueur au niveau de l'Etat.

Pour les informations non « classifiées », les systèmes d'exploitation et les logiciels utilisés doivent être mis à jour avec les derniers correctifs ne présentant pas de problème de compatibilité avec les configurations présentes, ni de régression fonctionnelle.

3 - Documentation des configurations des serveurs.

a -Configurations des serveurs de gestion

Les configurations mises en œuvre sur les serveurs de gestion de l'établissement, doivent être documentées et mises à jour, par le service informatique.

Ces documentations seront identifiées, localisées et tenues à disposition du RSSI.

b -Configurations des serveurs de recherche

Les configurations mises en œuvre sur les serveurs de recherche de l'établissement (serveurs hébergés dans les infrastructures gérées par le service informatique de l'établissement ou hébergées au sein de l'établissement, dans les locaux d'organismes de recherche) doivent être documentées et mises à jour par les organismes de recherche qui les utilisent.

Ces documentations seront identifiées, localisées et tenues à disposition du RSSI.

Un durcissement de ces serveurs hébergeant des données classifiées doit être effectué : principe de minimisation, principe de moindre privilège, principe de défense en profondeur et activité de veille et maintenance.

C - H abilitations : autorisations et contrôles d'accès.

L'accès aux ressources des systèmes d'information de l'établissement nécessite l'authentification des usagers, ainsi que le contrôle de leurs accès selon des droits déterminés par leurs fonctions ou besoin d'en connaître.

1 - Identification, authentification et contrôle d'accès logique

L'accès à toute ressource non publique nécessite 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. A cette fin, l'usage d'une carte à puce doit être privilégié.

Le contrôle d'accès doit être géré et s'appuyer sur un processus formalisé en cohérence avec la gestion des ressources humaines.

2 - 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),
- moindre privilège (chaque utilisateur accède aux ressources avec le minimum de privilèges lui permettant de conduire les actions explicitement autorisées pour lui).

3 - Gestion des profils d'accès aux applications

Les autorisations d'accès aux applications sont regroupées par profils de personnels utilisateurs, selon leurs fonctions.

Les applications de gestion tout comme les applications manipulant des données sensibles (au sens de « classifiées ») doivent permettre l'utilisation de ces profils d'accès.

Les principes du besoin d'en connaître et du moindre privilège s'appliquent.

4 - Autorisation d'accès des utilisateurs

Toute action d'autorisation d'accès d'un utilisateur à une ressource des systèmes d'information doit s'inscrire dans le cadre d'un processus d'autorisation formalisé, qui s'appuie sur le processus d'arrivée, de mutation interne et de départ du personnel, géré par la direction des ressources humaines.

5 - Revue et mises à jour des autorisations d'accès

Les autorisations d'accès sont maintenues à jour par les responsables de services, au fur et à mesure des changements de fonction des personnels qu'ils encadrent. La direction des ressources humaines participe à ce processus de mise à jour.

6 - Confidentialité des informations d'authentification.

Les informations d'authentification (mots de passe d'accès aux systèmes d'information, clés privées liées aux certificats électroniques...) sont considérées comme des données sensibles.

7 - Gestion des mots de passe

Les utilisateurs ne doivent pas stocker leurs mots de passe en clair (c'est-à-dire non chiffré) sur leur poste de travail. Les mots de passe ne doivent pas transiter en clair sur les réseaux.

8 - Initialisation des mots de passe

Chaque compte utilisateur doit être créé avec un mot de passe initial aléatoire unique. La fourniture du premier mot de passe à l'utilisateur doit être encadrée par un processus sécurisé.

9 - Politiques de mots de passe

Les règles de gestion et de protection des mots de passe, édictées par l'université et donnant accès aux applications et infrastructures, doivent être respectées dans chaque entité de l'établissement.

La politique de mots de passe de l'établissement prendra en compte les recommandations de l'ANSSI.

10 - Contrôle systématique de la qualité des mots de passe.

L'utilisateur choisit des mots de passe sécurisés (respect d'au moins trois critères sur les quatre cités) :

- 8 caractères minimum, dont au moins : une majuscule, une minuscule, un chiffre et un caractère spécial (!-{[|@...), noté sur les codes PIN Smartphone ;
- l'utilisateur change ses mots de passe régulièrement, et au minimum tous les 6 mois ;
- il les garde secrets et s'oblige à les mémoriser ;
- il s'interdit de noter ses mots de passe sur papier ou dans un fichier non protégé.

11 - Utilisation de certificats électroniques

L'utilisation de certificats électroniques doit respecter les règles édictées par le référentiel général de sécurité (RGS).

12 - Contrôle systématique de la Qualité des mots de passe

Un système de gestion informatique des mots de passe fournit les moyens techniques permettant d'imposer la politique de mots de passe et de vérifier son application.

Un contrôle périodique des paramètres techniques relatifs aux mots de passe est réalisé par le RSSI.

13 - Séquestre des authentifiants « administrateurs ».

Les authentifiants permettant l'administration des ressources des systèmes d'information doivent être placés sous séquestre et tenus à jour, dans un coffre ou une armoire fermée à clé. Un outil sécurisé de gestion centralisée des mots de passe pourra être utilisé. L'authentifié doit être informé de l'existence de ces opérations de gestion, de leurs finalités et limites. 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 (notamment carte à puce) 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.

14 - Politique de mots de passe « administrateurs »

Chaque administrateur doit disposer d'un mot de passe propre et destiné à l'administration.

15 - Gestion du départ d'un administrateur des SI

En cas de départ d'un administrateur disposant de privilèges sur des composants des systèmes d'information, les comptes individuels dont il disposait doivent être immédiatement désactivés.

Les éventuels mots de passe d'administration dont il avait connaissance doivent être changés (mots de passe des comptes fonctionnels, comptes génériques ou comptes de service utilisés dans le cadre des fonctions de l'administrateur...).

D - Sécurisation de l'exploitation.

Objectif : fournir aux administrateurs les outils nécessaires à l'exercice des tâches SSI et configurer ces outils de manière sécurisée.

1 - Restriction des droits

Sauf exception dûment motivée et validée par le RSSI, les utilisateurs n'ont pas de droit d'administration. Ainsi, les personnels administratifs ne sont pas administrateurs de leur poste de travail.

Par dérogation, les personnels effectuant des enseignements peuvent posséder les droits d'administration sur les machines des salles de cours de l'établissement, afin de répondre à un besoin pragmatique et fonctionnel, lié à leurs tâches. Dans ce cas précis, ces machines doivent se situer dans un Vlan isolé.

2 - 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.

3 - Habilitation des administrateurs

Au sein de l'établissement : tous les personnels du service informatique ont vocation à être habilités pour les accès avec privilèges d'administrateurs, selon leurs domaines de compétences techniques et selon leurs fonctions. Ces habilitations sont validées par l'AQSSI ou le RSSI.

Le RSSI dispose, par lettre de missions, de l'accès à la totalité des systèmes d'information de l'établissement, avec la totalité des droits d'accès administrateurs.

Par dérogation validée par l'AQSSI ou le RSSI, les droits d'accès avec privilèges d'administrateurs, peuvent être conférés à un personnel n'appartenant pas au service informatique, pour nécessités de service.

Une charte administrateur devra être soumise aux administrateurs précisant leurs droits et devoirs dans l'exercice de leur fonction ou de leur activité professionnelle. Elle précise le cadre légal,

réglementaire et déontologique dans lequel doivent s’inscrire les actions d'administration des systèmes d'information.

4 - Gestion des actions d'administration

Les opérations d'administration doivent être tracées de manière à pouvoir gérer au niveau individuel l'imputabilité des actions d'administration, au mieux du possible et de l'état de l'art.

5 - Sécurisation des flux d'administration

Les opérations d'administration sur les ressources de l'établissement doivent s'appuyer sur des protocoles sécurisés. Un réseau dédié à l'administration des équipements, ou au moins un réseau séparé logiquement (utilisation de Vlans) de celui des utilisateurs, doit être utilisé.

6 - Centraliser la gestion des systèmes d'information.

Afin de gérer efficacement un grand nombre de postes d'utilisateurs, de serveurs ou d'équipements réseau, les administrateurs doivent utiliser des outils centralisés, permettant l'automatisation de traitements quotidiens et offrant une vue globale et pertinente sur les systèmes d'information.

7 - Sécurisation des outils de prise de main à distance

La prise de main à distance d'une ressource informatique des systèmes d'information de l'établissement ne doit être réalisable que par les agents autorisés au sein du service informatique.

8 - Définir une politique de gestion des comptes du domaine

Une politique explicite de gestion des comptes du ou des domaines de l'établissement doit être documentée.

9 - 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 (attaque par dictionnaire). Une complexité minimale dans le choix des mots de passe des utilisateurs doit être mise en place et maintenue à un niveau suffisant en regard des menaces à parer.

10 - 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.

11 - Restreindre au maximum l'appartenance aux groupes d'administration du domaine

L'appartenance aux groupes du domaine ADMINISTRATEURS DE L'ETABLISSEMENT 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.

12 - Maîtriser l'utilisation des comptes de service

Les mots de passe des comptes de service sont souvent inscrits directement (« *en dur* ») dans des applications ou dans des systèmes. L'utilisation de ces comptes de services doit être déterminée, afin d'être en mesure de changer ces mots de passe en urgence.

13 - Limiter les droits des comptes de service

Les comptes de service doivent détenir le minimum de droits nécessaires pour accomplir les tâches qui leur sont liées. Cette restriction des droits doit s'appliquer selon le principe du moindre privilège.

14 - Désactiver les comptes du domaine obsolètes

Les comptes devenus obsolètes, que ce soient des comptes d'utilisateur (administrateur, de service ou utilisateur standard) ou des comptes de machine, doivent être désactivés ou supprimés dès leur obsolescence avérée.

15 - Supprimer les comptes génériques

Les comptes génériques ne doivent plus être créés. Les comptes génériques déjà existants, doivent au fur et à mesure être remplacés par des comptes nominatifs.

16 - Améliorer la gestion des comptes d'administrateur locaux

La réutilisation des empreintes numériques d'un compte utilisateur local, d'une machine à une autre, ne doit pas être possible.

Pour ce faire, soit des mots de passe différents seront utilisés pour les comptes locaux d'administration, soit la connexion à distance via ces comptes sera interdite.

17 - Maintenance externe

Les données non chiffrées doivent être effacées avant l'envoi en maintenance externe de toute ressource informatique. Les opérations de chiffrement doivent faire appel à des produits qualifiés par l'Etat (ANSSI). L'effacement des données sensibles doit s'appuyer sur des produits qualifiés, ou respecter des procédures établies en concertation avec l'ANSSI.

Lors de réparation de serveurs, les supports de données (disques durs...) sont conservés par l'établissement, par contrat.

18 - Mise au rebut

Lorsqu'une ressource informatique doit quitter définitivement l'établissement, les données présentes sur les supports de données (disques durs, 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.

19 - Protection contre les codes malveillants - Antivirus

Des logiciels de protection contre les codes malveillants (antivirus...) doivent être installés sur l'ensemble des serveurs et postes de travail de l'établissement. Les analyses de leurs journaux doivent être corrélées.

20 - Gestion des événements de sécurité de l'antivirus

Les journaux des événements de sécurité du ou des logiciels antivirus doivent être centralisés sur un serveur, pour analyse statistique et gestion des problèmes *a posteriori.*

21 - 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 par un dispositif validé par le RSSI.

22 - Configuration du navigateur Internet

Les navigateurs déployés par le service informatique sur l'ensemble des serveurs et des postes de travail nécessitant un accès internet ou intranet, doivent être configurés de manière sécurisée

(désactivation des services inutiles, nettoyage du magasin de certificats...) et être maintenus à jour vis-à-vis des correctifs de sécurité.

23 - Définir et mettre en œuvre une politique de suivi et d'application des correctifs de sécurité

Le maintien dans le temps du niveau de sécurité des systèmes 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 suivant les contraintes et le niveau d'exposition du système.

24 - Déploiement des correctifs de sécurité

Les correctifs de sécurité des ressources informatiques de l'établissement doivent être déployés par les équipes qui en ont la charge (par pôle, par site ou par autre entité fonctionnelle).

25 - Assurer la migration des systèmes obsolètes

L'ensemble des logiciels utilisés dans les systèmes d'information de l'établissement doit être dans une version pour laquelle l'éditeur assure le support, et tenu à jour, sauf dérogation explicite validée par l'AQSSI ou le RSSI.

En cas de défaillance du support, il convient d'en étudier l'impact et de prendre les mesures adaptées.

26 - Isoler les systèmes obsolètes restants

Il est nécessaire d'isoler les systèmes obsolètes, 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 (filtrage strict), des éléments d'authentification (qui ne doivent pas être communs avec le reste des systèmes d'information) et des applications (pas de ressources partagées avec le reste des systèmes d'information).

27 - 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, pendant la durée légale.

28 - Définir et mettre en œuvre une politique de gestion et d'analyse des journaux de traces.

Une politique de gestion et d'analyse des journaux de traces des événements de sécurité est définie par le RSSI, validée par l'autorité qualifiée (AQSSI), 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.

29 - 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.

30 - Anticipation des attaques

En complément de la prévention, les attaques peuvent être prévenues, atténuées ou neutralisées dans leurs effets afin de permettre de prendre les dispositions propres à la poursuite de l'activité.

Pour ce faire, mettre en œuvre un ensemble d'éléments techniques, de type SIEM, sondes etc., permettant l'anticipation des attaques sur le réseau.

E - Défense des systèmes d'information.

1 - 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 des systèmes d'information et à la surveillance des flux d'entrée et de sortie des systèmes d'information.

2 - Maîtrise des matériels

Les postes de travail gérés par le service informatique de l'établissement (y compris dans le cas d'une location) sont fournis à l'utilisateur avec une configuration standard.

La connexion d'équipements non maîtrisés, non administrés ou non mis à jour par le service informatique (qu'il s'agisse d'ordiphones, d'équipements informatiques nomades et fixes ou de supports de stockage amovibles) sur les réseaux professionnels de l'établissement est interdite, sauf dérogation explicite.

3 - Rappel des mesures de protection contre le vol

Les postes fixes bénéficient des mesures de protection physique offertes au titre de la directive de sécurité physique de la présente PSSI. Chaque utilisateur doit veiller à la sécurité des supports

amovibles (clés USB et disques amovibles), notamment en les conservant dans un endroit sûr. Les données contenues sur ces supports doivent être chiffrées. Les supports contenant des données sensibles doivent être stockés dans des meubles fermant à clef.

4 - Déclarer les pertes et vols

Toute perte ou vol d'une ressource de système d'information doit être déclarée au RSSI.

5 - Réaffectation de matériels informatiques

Une procédure de gestion des postes et supports dans le cadre de départs de personnel ou de réaffectations à de nouveaux utilisateurs doit être mise en place par le service informatique et validée par le RSSI. Elle doit définir les conditions de recours à un effacement des données.

6 - Déclaration des équipements nomades aptes à traiter des informations sensibles

L'autorité d'homologation des systèmes d'information, à défaut l'AQSSI ou le RSSI, valide les usages possibles des équipements nomades vis-à-vis du traitement des informations sensibles ; les usages non explicitement autorisés sont interdits.

7 - Accès à distance aux systèmes d'information de l'établissement.

Les utilisateurs distants doivent s'authentifier sur le réseau de l'établissement en utilisant une méthode conforme à l'annexe B3 du RGS.

8 - Impression des informations sensibles.

Les impressions d'informations sensibles doivent être effectuées selon une procédure prédéfinie, garantissant le contrôle de l'utilisateur, du déclenchement de l'impression jusqu'à la récupération du support imprimé.

Pour ce faire, l'utilisateur doit s'authentifier sur l'imprimante, à l'aide de sa carte AMU, avant de pouvoir lancer son impression.

9 - Sécurité des imprimantes et copieurs multifonctions.

Les imprimantes et copieurs multifonctions sont des ressources informatiques à part entière qui doivent être gérées en tant que telles. Leur communication avec le réseau extérieur de l'établissement doit être définie et sécurisée.

F - Exploitation sécurisée des ressources informatiques.

1 - 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. Seuls les services et applications nécessaires sont installés (réduction de la surface d'attaque). Les comptes administrateurs doivent être traités de façon suivie et sécurisée au maximum, en regard de l'état de l'art.

2 - Logiciels en Tiers Présentation

La mise en œuvre d'une configuration renforcée est obligatoire sur les logiciels déployés pour le « tiers présentation » (ex : serveur Web, Reverse Proxy).

3 - Logiciels en Tiers Application

Des règles de développement sécurisé et les configurations des logiciels en « Tiers Application » doivent être fixées et appliquées. Elles sont détaillées dans le cadre de cohérence technique (CCT).

4 - Logiciels en Tiers Données

Des règles strictes (restrictions d'accès, interdictions de connexion, gestion des privilèges) s'appliquent aux logiciels en tiers données. Ces règles doivent être détaillées dans le cadre de cohérence technique (CCT).

5 - Passerelle d'échange de fichiers

Les échanges de fichiers entre applications doivent privilégier les protocoles sécurisés (SSL/TLS, FTPS...), au mieux du possible en regard de l'état de l'art.

6 - Messagerie utilisateur

La redirection de messages professionnels vers une messagerie personnelle est à proscrire car cela constitue une fuite irrémédiable d'informations de l'entité. Si nécessaire des moyens maîtrisés et sécurisés pour l'accès distant à la messagerie professionnelle doivent être utilisés.

7 - Messagerie technique

Pour satisfaire les besoins d'exploitation et de supervision des infrastructures et des applications, une messagerie dite « technique » peut être déployée, en interne au service informatique de

l'établissement. Cette messagerie technique ne doit être, en aucun cas, utilisée directement par un utilisateur.

8 - Filtrage des flux applicatifs

Des mécanismes de filtrage et de cloisonnement doivent être mis en œuvre afin de garantir un niveau de sécurité satisfaisant face aux attaques informatiques, en regard de l'état de l'art.

9 - Flux d'administration

Deux types de flux d'administration sont à distinguer :

- les flux d'administration de l'infrastructure (réservés aux agents du service informatique) d'une part,
- les flux d'administration des applications métier (réservés à la direction métier) d'autre part.

L'attribution des droits d'administration doit respecter cette différenciation et les deux types de flux d'administration doivent être dans la mesure du possible cloisonnés.

10 - Service de noms de domaine - DNS technique

Dans le cas du déploiement d'un serveur de noms de domaines « technique », pour des besoins liés à des informations de sensibilité importante, les extensions sécurisées DNSSEC seront mises en œuvre (d'un niveau minimum : NSEC3).

11 - Effacement de support

Le reconditionnement et la réutilisation de supports de stockage (disques durs...) pour un autre usage (ex: réattribution d'une machine/serveur) ne sont autorisés qu'après une opération d'effacement sécurisé des données.

12 - Destruction de support

La fin de vie d'un support ou d'un matériel embarquant un support de stockage (imprimante, routeur, commutateur...) doit s'accompagner d'une opération d'effacement sécurisé des données ou bien d'une destruction de ce support (disque dur, mémoire morte...) avant remise au constructeur ou sortie d'inventaire / mise au rebut.

13 - Traçabilité / imputabilité

Afin d'assurer une cohérence dans les échanges entre applications ainsi qu'une traçabilité pertinente des événements techniques et de sécurité, les infrastructures de serveurs emploient une référence de temps commune (service NTP, Network Time Protocol).

14 - Supervision

Un cloisonnement entre les flux de supervision (remontée d'informations) et les flux d'administration (commandes, mises à jour) doit être mis en place.

15 - Accès aux périphériques amovibles

L'accès aux supports informatiques amovibles fait l'objet de procédures particulières de sécurité (utilisation, stockage, mise au rebut), notamment lorsqu'ils contiennent de l'information sensible ou lorsqu'ils sont utilisés pour des opérations d'exploitation ou encore lorsqu'ils ont contenu de telles informations.

16 - Conservation et de destruction des informations à protéger

Certaines catégories d'informations nécessitent des conditions de conservation et de destruction adaptées. Les mesures sont adaptées à l'environnement propre à l'AMU et doivent demeurer cohérentes entre elles.

En particulier, le contrôle préalable des bonnes conditions de stockage revêt un aspect fondamental dès lors que l'information est confiée contractuellement à l'AMU. Des normes précises doivent être adoptées pour l'élimination de l'information périmée qui conserve un caractère résiduel de confidentialité.

De plus, l'archivage de documents magnétiques fait l'objet d'obligations juridiques en termes de durée de conservation et de protection des supports, selon la nature des informations concernées (informations comptables ou fiscales, relatives au personnel…).

La protection des supports papier (listing, documentation, impression de rapports…) est souvent délaissée, bien qu'ils contiennent des informations de l'organisme.

Les supports doivent être protégés conformément aux règles associées à la classification des informations qu'ils hébergent. Ainsi, il doit exister, en fonction de la classification, des règles de sécurité concernant la gestion, le contrôle, le stockage (contre le vol et la destruction), le transport et la mise au rebut des supports.

17 - Accès aux réseaux

Au niveau des salles machines informatiques, ainsi qu'au niveau de l'exploitation des ressources informatiques de l'établissement, 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.

18 - Audit/contrôle

Le RSSI pilote des audits réguliers des systèmes d'information relevant de sa responsabilité.

X - Sécurisation du Système d'information

A - Sécurité du réseau

L'administration du réseau de l'établissement est placée sous la responsabilité de son service informatique.

1 - Sécurité des accès au réseau

L'accès au réseau de l'université n'est effectif qu'après authentification de l'utilisateur (personnels de l'université ou partenaires).

Ces accès doivent être journalisés.

La protection des systèmes d'information s'opère par la mise en œuvre de filtres d'accès, appliqués sur les équipements en tête de réseau, et gérant :

- les accès externes et internes au réseau de l'université,
- les flux réseaux entrants et les flux réseaux sortants des systèmes d'information.

L'accès réseau depuis l'extérieur, aux postes de travail, doit être une exception justifiée en termes de nécessités de service en vue d'accomplir des tâches particulières et identifiées, validées d'une part, par le responsable de l'entité dans laquelle ce poste de travail est installé et d'autre part, par le directeur du service informatique ou par le RSSI.

La définition des filtres d'accès réseau régissant les flux réseau entrants doit être systématiquement de type : « tout ce qui n'est pas autorisé explicitement est interdit ».

2 - Sécurité des accès aux serveurs via le réseau

Les accès réseau aux serveurs doivent être filtrés vis-à-vis des postes de travail.

Les accès réseau entre les serveurs doivent être filtrés :

La politique de gestion des accès aux serveurs sera particulière pour :

-les serveurs accessibles uniquement à partir du réseau de l'Université d'Aix-Marseille,

-les serveurs accessibles depuis l'extérieur. Ceux-ci seront protégés de façon « durcie », selon les termes de l'ANSSI (outils d'analyse des traces, de métrologie…). Les matériels nomades de l'université auront accès à ces serveurs depuis l'extérieur, en utilisant des connexions chiffrées, par réseau privé virtuel (VPN).

La définition des filtres d'accès aux réseaux de serveurs, régissant les flux réseau entrants et sortants, doit être systématiquement de type : « tout ce qui n'est pas autorisé explicitement est interdit ».

3 - Sécurité des accès au réseau sans-fil

La sécurité de l'accès au réseau sans-fil de l'université doit être l'objet d'une politique spécifique d'autorisations :

- le système d'information de l'université n'est pas accessible via ce réseau,
- l'accès au réseau de l'université n'est effectif qu'après authentification de l'utilisateur (personnels de l'université, partenaires...),
- les accès doivent être journalisés.

Les matériels nomades doivent être surveillés de façon particulière avant et lors de leur connexion au réseau de l'université afin d'éviter l'introduction de programmes malveillants.

B - Usage sécurisé des réseaux nationaux.

1 - Systèmes autorisés sur le réseau

Seuls les équipements gérés et configurés par les équipes informatiques habilitées peuvent être connectés au réseau local de l'université, sauf exception, dans le cas d'un contrat passé entre l'établissement et une société.

2 - Interconnexion avec des réseaux externes

Toute interconnexion entre les réseaux locaux de l'établissement ou d'une de ses entités (site géographique, service, laboratoire, structure d'enseignement/recherche, entreprise hébergée...) et d'un réseau externe (réseau d'un tiers, internet, etc.) doit être réalisée via les infrastructures réseau validées par l'établissement.

3 - Mettre en place un filtrage réseau pour les flux sortants et entrants

Les connexions des machines du réseau de l'établissement (donc de tous ses sites géographiques), vers l'extérieur doivent être filtrées par un dispositif de type pare-feu.

4 - Protection des informations

Les accès à internet passent obligatoirement par des passerelles validées par l'établissement ou par des accords nationaux ministériels, sur des réseaux autorisés via des accords officiels.

Dès lors que des informations sensibles doivent transiter sur des réseaux non maîtrisés, elles doivent être protégées par un chiffrement adapté.

C - Usage sécurisé des réseaux locaux.

1 - Cloisonner le SI en sous-réseaux de niveaux de sécurité homogènes

Les systèmes d'information doivent être segmentés selon des zones présentant chacune un niveau de sécurité homogène. Cette segmentation sera mise en œuvre par l'utilisation de matériels qui permettront une déconnexion physique des réseaux en cas d'incidents particuliers.

2 - Interconnexion des sites géographiques.

L'interconnexion des différents sites géographiques de l'université doit être réalisée au-travers de connexions sécurisées et utilisant les règles de sécurité des réseaux définies pour l'ensemble de l'établissement par le service informatique et validées par le RSSI.

3 - Cloisonnement des ressources en cas de partage de locaux.

Dans le cas où une entité interne à l'établissement (service, laboratoire...) partage des locaux (bureaux ou locaux techniques) avec des entités externes à l'établissement (entreprises, prestataires de services...), des mesures de cloisonnement des ressources informatiques doivent être mises en place. Si le cloisonnement n'est pas physique, les mesures prises doivent être validées par le RSSI de l'établissement.

D - Accès spécifiques à internet.

1 - Cas particulier des accès spécifiques dans une entité

Les accès spécifiques à internet nécessitant des droits particuliers pour un usage métier ne peuvent être mis en place que sur dérogation dûment justifiée et sur des machines identifiées.

E - Usage sécurisé des réseaux sans fil.

1 - Mise en place de réseaux sans fil

Le déploiement de réseaux sans fil doit faire l'objet d'une **analyse de risques spécifique**.

Ces réseaux doivent faire l'objet de mesures de défense en profondeur. En particulier, une segmentation du réseau doit être mise en place afin de limiter à un périmètre déterminé, les conséquences d'une intrusion depuis la voie hertzienne.

À défaut de mise en œuvre de mesures spécifiques, le déploiement de réseaux sans fil sur des systèmes d'information manipulant des données sensibles est proscrit.

F - Sécurité des mécanismes de commutation et de routage.

1 - Implanter des mécanismes de protection contre les attaques sur les couches basses.

L'implantation des protocoles de couches basses doit être particulièrement sécurisée afin de se prémunir contre les attaques par saturation ou empoisonnement de cache, notamment.

2 - 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'incident.

3 - Configurer le protocole IGP de manière sécurisée

En cas d'utilisation d'un protocole de type IGP : ce protocole de routage dynamique doit être activé exclusivement sur les interfaces nécessaires à la construction de la topologie du réseau et désactivé sur le reste des interfaces. La configuration du protocole de routage dynamique doit systématiquement s'accompagner d'un mot de passe de type MESSAGE-DIGEST-KEY.

4 - Sécuriser les sessions EGP

L'utilisation d'un protocole de type EGP doit être évitée.

5 - Modifier systématiquement les éléments d'authentification par défaut des équipements et services

Les mots de passe par défaut doivent être modifiés, tout comme les certificats, lors de la mise en exploitation des matériels réseau.

Les matériels réseau acquis par l'établissement doivent permettre de modifier les certificats installés par défaut.

6 - Durcir les configurations des équipements de réseaux

Les équipements des réseaux (ex. 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 du plan de contrôle.

G - Cartographie réseau.

1 - Elaborer les documents d'architecture technique et fonctionnelle

L'architecture réseau du système d'information doit être décrite et formalisée par des schémas d'architecture et des configurations, maintenus à jour des évolutions apportées aux systèmes d'information de l'établissement. Les documents d'architecture sont sensibles et font l'objet d'une protection adaptée. La cartographie réseau s'insère dans la cartographie globale des systèmes d'information.

H - Contrôle d'accès aux systèmes d'information - Habilitations

Les systèmes d'information de l'établissement ne sont accessibles que par la validation des droits et autorisations d'un utilisateur, via un processus d'identification et d'authentification.

Cette authentification doit se faire par l'annuaire informatique (ex. Active Directory) de l'établissement.

Les droits d'accès attribués à un utilisateur ne doivent être que ceux uniquement nécessaires à l'accomplissement de ses tâches en regard de ses fonctions.

Cette attribution de droits d'accès doit être validée par le responsable des données accédées.

L'utilisation d'un compte utilisateur par plusieurs personnels est une exception qui doit être justifiée par des nécessités de service fonctionnelles.

Ces comptes utilisateurs partagés doivent être répertoriés et leur liste doit être mise à jour régulièrement.

Les accès au réseau et au système d'information doivent être journalisés.

I - Administration des postes de travail

L'administration des postes de travail des entités dépendant uniquement de l'établissement (c'est-àdire non sous plusieurs tutelles) est placée sous la responsabilité de son service informatique, sauf dispositions contraires spécifiques.

L'administration de leur poste de travail par des personnels eux-mêmes est une exception qui doit être justifiée par des nécessités de service particulières.

L'assistance informatique, les administrateurs systèmes et réseaux de l'établissement, sont autorisés à prendre le contrôle à distance des matériels informatiques, afin de réaliser des opérations de maintenance sur le poste de travail d'un utilisateur, en le prévenant au-préalable, dans le respect des lois « Informatique et Libertés ».

La prise de main à distance sur un poste de travail par un prestataire, doit être réalisée avec une solution sécurisée validée par le RSSI.

J - Sécurisation des postes de travail, des matériels nomades et de la téléphonie

1 - Sécurisation des postes de travail

La sécurisation des postes de travail financés par l'université (matériels fixes ou nomades) des entités dépendant uniquement de l'établissement (c'est-à-dire non sous plusieurs tutelles) est placée sous la responsabilité de son service informatique, sauf dispositions contraires spécifiques.

La sécurisation des postes de travail non financés par l'université (matériels fixes ou nomades), d'une entité de l'établissement, est placée sous la responsabilité du responsable hiérarchique de cette entité, sauf dispositions contraires spécifiques.

Dans tous les cas :

- la PSSI de l'université s'applique (cf. « Chaîne de responsabilités de la SSI au sein de l'université »),
- l'accès aux postes de travail (fixes ou nomades) s'effectue en utilisant un mot de passe robuste,
- un mot de passe demeure confidentiel et personnel. Il est interdit de le divulguer à un tiers, quel qu'il soit et ne doit pas être laissé sans protection (exemple : écrit sur un Post-It ou encore sous le clavier…),
- les utilisateurs doivent laisser se mettre en œuvre correctement les applicatifs de sécurisation installés sur leurs matériels informatiques de travail (mises à jour : de l'antivirus, du système d'exploitation, des applications ; remontées d'informations SSI…).

Les postes de travail nomades devront faire l'objet de mesures de sécurité particulières : chiffrement du ou des disques durs (en totalité ou en partie contenant des données sensibles et/ou relatives à l'établissement), protection contre le vol etc. Dans le cas de voyages hors du territoire national, des mesures de sécurité adaptées aux pays visités devront être mises en œuvre (certains pays ne tolèrent pas la présence de partitions chiffrées sur les disques durs : d'autres solutions pourront être mises en œuvre).

Lorsque l'unité centrale d'un poste fixe est peu volumineuse (donc facilement emportée), elle doit être protégée contre le vol par un système d'attache (par exemple un câble antivol).

Un câble physique de sécurité doit être fourni avec chaque poste portable. Les utilisateurs doivent être sensibilisés à son utilisation.

Une procédure SSI définit les règles concernant le traitement à appliquer aux informations ayant été stockées ou manipulées sur les postes réaffectés.

La gestion des privilèges des utilisateurs sur leurs postes de travail doit suivre le principe du « moindre privilège » : chaque utilisateur ne doit disposer que des privilèges nécessaires à la conduite des actions relevant de sa mission.

Les privilèges d'accès « administrateur » doivent être utilisés uniquement pour les actions d'administration le nécessitant, sauf dispositions contraires validées par le RSSI.

L'accès au compte « 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.

Lorsque cela s'avère possible, les données traitées par les utilisateurs doivent être stockées sur des espaces réseau, eux-mêmes sauvegardés selon les exigences de l'établissement ou des entités et en accord avec les règles de sécurité en vigueur.

Dans le cas où des données doivent être stockées en local sur le poste de travail, les utilisateurs doivent mettre en œuvre les moyens de synchronisation ou de sauvegarde fournis par l'établissement ou par leur entité de recherche.

Le partage de répertoires ou de données hébergées localement sur les postes de travail n'est pas autorisé.

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 ».

Une solution de chiffrement labellisée doit être mise à 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.

Les accès à distance aux SI de l'entité (accès dits « nomades ») doivent être réalisés via des infrastructures sécurisées et identifiées par l'établissement. Lorsque l'accès à distance utilise d'autres infrastructures, l'usage de réseaux privés virtuels (VPN) de confiance est de toute façon nécessaire.

Un pare-feu local conforme aux exigences SSI de l'établissement doit être installé sur les postes nomades.

Le stockage local d'information sur les postes de travail nomades doit être limité au strict nécessaire. Les informations sensibles doivent être obligatoirement chiffrées par un moyen de chiffrement labellisé.

Pour les postes de travail nomades manipulant des données sensibles, un filtre de confidentialité doit être fourni et être positionné sur l'écran dès lors que le poste est utilisé en dehors de l'entité.

La configuration des interfaces de connexion sans fil doit interdire les usages dangereux de ces interfaces.

Des règles de configuration des interfaces de connexion sans fil (Wifi, Bluetooth, 3G….), permettant d'interdire les usages non maîtrisés et d'éviter les intrusions via ces interfaces, doivent être définies et

appliquées. Les interfaces sans fil ne doivent être activées qu'en cas de besoin et non systématiquement.

Il doit être appliqué un contrôle de l'usage des ports USB sur les postes de travail, notamment sur les postes « sensibles », interdisant par exemple la copie de l'ensemble des données contenues dans un fichier.

Un outil de vérification régulière de la conformité des éléments de configuration des postes de travail doit être mis en place, afin d'éviter une dérive dans le temps de ces éléments de configuration. Les informations afférentes pourront être utilisées dans le cadre d'un indicateur du tableau de bord de la SSI de l'établissement.

2 - Sécurisation de la téléphonie

Les autocommutateurs doivent être maintenus à jour au niveau des correctifs de sécurité.

Leur configuration doit être durcie.

La définition et l'affectation des droits d'accès et des privilèges aux utilisateurs (transfert départdépart, entrée en tiers, interphonie, autorisation de déblocage, renvoi sur numéro extérieur, substitution, substitution de privilège, interception d'appel dirigé...) doivent faire l'objet d'une attention particulière. Une revue de la programmation téléphonique doit être organisée périodiquement.

Les utilisateurs doivent être sensibilisés au besoin de modifier le code d'accès de leur téléphone et de leur messagerie vocale.

Les appareils mobiles (téléphones portables, tablettes, etc.) doivent être maîtrisés par l'établissement et être intégrés dans un outil de gestion des terminaux mobiles. Cela permet d'harmoniser et de sécuriser la flotte de l'établissement en s'assurant notamment de la bonne propagation de patchs de sécurités.

Des postes téléphoniques filaires doivent être attribués aux utilisateurs dont les échanges sont les plus sensibles (les communications réalisées au travers du protocole DECT sont susceptibles d'être interceptées, même si les mécanismes d'authentification et de chiffrement que propose ce protocole sont activés).

3 - Sécurisation de l'impression

Les imprimantes et copieurs multifonctions hébergés au sein de l'établissement doivent faire l'objet d'un durcissement en termes de sécurité :

- changement des mots de passe initialement fixés par le « constructeur »,
- désactivation des interfaces réseau inutiles,
- suppression des services inutiles,
- chiffrement des données sur le disque dur lorsque cette fonctionnalité est disponible, – configuration réseau statique.

4 - Sécurisation de la numérisation

Lorsqu'elle est activée, la fonction de numérisation sur les copieurs multifonctions hébergés dans l'établissement doit être sécurisée par la mise en œuvre, *a minima*, des mesures de sécurité suivantes :

- envoi de documents uniquement à destination d'une adresse de messagerie interne à l'établissement, voire à la ZRR,
- envoi uniquement à une seule adresse de messagerie.

K - Administration des serveurs

L'administration des serveurs de gestion de l'établissement est placée sous la responsabilité de son service informatique, sauf dispositions contraires spécifiques.

L'administration des serveurs de recherche d'une entité de l'établissement, est placée sous la responsabilité du responsable hiérarchique de cette entité, sauf dispositions contraires spécifiques.

Dans tous les cas, la PSSI de l'université s'applique (cf. « Chaîne de responsabilités de la SSI au sein de l'université »).

L - Sécurité des applications et des développements

Tout projet informatique participant aux systèmes d'information, réalisé en interne à l'établissement ou développé par un prestataire externe, doit être validé au niveau sécurité, lors de chacune de ses étapes de développement.

Cette validation sera accordée suite à l'étude d'un dossier de sécurité, dans lequel il sera indiqué pour chaque projet informatique : les objectifs visés, les méthodes de développement employées, les mesures de sécurité mises en œuvre.

Le passage en production d'un projet informatique ne peut être effectif qu'après validation de son dossier sécurité.

Cette validation doit être approuvée par le RSSI, voire le Président de l'Université d'Aix-Marseille (en tant qu'AQSSI) en fonction de l'importance de l'application dans les systèmes d'information ou de la sensibilité des données traitées.

Le degré de sécurité exigé pour une application sera fonction de la sensibilité des données traitées. Les informations techniques sur les logiciels utilisés ne seront diffusées qu'au strict minimum requis par les nécessités de fonctionnement.

Lorsqu'une application doit stocker les mots de passe de ses utilisateurs, des mesures seront mises en œuvre pour se prémunir contre les attaques documentées (attaques par dictionnaire, attaques par tables arc-en-ciel, attaques par force brute...).

Le fonctionnement des applications développées devra être le plus indépendant possible de son environnement logiciel et matériel : la portabilité des développements sera favorisée au maximum (vérification en phases de conception et de spécification technique).

La sécurité sera intégrée à toutes les étapes du cycle de vie 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.

Les développements Web seront effectués en cohérence avec les référentiels de sécurité (règles de bonnes pratiques, à l'usage des développeurs). Les applications à risques seront protégées par la mise en place d'une filtration tierce.

Toute initiative locale (ex. une structure d'enseignement/recherche) de développement informatique doit respecter les exigences nationales en matière de SSI, concernant la prise en compte de la sécurité dans les projets et les développements informatiques.

M - Interventions de sociétés prestataires de services, télémaintenances externes

Des sociétés prestataires de services peuvent être amenées à effectuer plusieurs types d'actions, via des accès internes ou externes à l'université :

- gestion de matériels,
- gestion de serveurs au niveau système,
- gestion d'applications.

Il est nécessaire de formaliser les relations entre ces sociétés et l'université, par des contrats, qui stipuleront :

- les conditions d'accès au réseau, aux serveurs, aux systèmes d'information,
- les droits d'accès aux ressources informatiques, attribués,
- les responsabilités des partenaires,
- l'imputabilité des problèmes en cas d'incidents.

Afin de garantir la SSI et le périmètre d'intervention des sociétés de services, les actions de ces prestataires doivent être encadrées au mieux des possibilités techniques disponibles au moment de leurs interventions

La gestion d'un composant sensible des systèmes d'information, par un prestataire de services externe à l'université, est interdite, sauf dispositions contraires spécifiques, validées soit par le RSSI, soit par le Président de l'Université d'Aix-Marseille (en tant qu'AQSSI), en fonction du degré de sensibilité des informations traitées.

En cas de sous-traitance de développement logiciel, la rédaction du contrat entre l'établissement et le(s) prestataire(s) devra intégrer plusieurs clauses relatives à la SSI :

- les développeurs devront avoir été formés sur le développement sécurisé et sur les vulnérabilités classiques ;
- utilisation obligatoire d'outils permettant de minimiser les erreurs introduites durant le développement (outils d'analyse statique de code, utilisation de bibliothèques réputées pour leur sécurité...) ;
- production d'une documentation technique décrivant l'implantation des protections développées (gestion de l'authentification, stockage des mots de passe, gestion des droits, chiffrement...) ;
- respect de normes de développement sécurisé, qu'elles soient propres au développeur, publiques ou propres au commanditaire ;
- obligation pour le prestataire de corriger, dans un temps raisonnable à définir et pour un prix déterminé, les vulnérabilités introduites durant le développement et qui lui sont remontées,

  en incluant automatiquement les corrections des autres occurrences des mêmes vulnérabilités.

XI - Evaluation et maintien du niveau effectif de sécurité

Le niveau de sécurité des systèmes d'information est en évolution perpétuelle. Il dépend de mécanismes dynamiques, qui permettent son maintien, voire son augmentation (mise à jour : des matériels, des logiciels gérant les matériels, des systèmes d'exploitation, des antivirus, des applications…).

A cette fin, le RSSI supervise les mesures techniques qui sont à prendre pour le maintien du niveau de sécurité des systèmes d'information (politique : de mises à jour, d'analyse de journaux, de suivi des vulnérabilités signalées…).

A - Audits

Des audits pourront être réalisés afin d'étudier les niveaux de sécurité des différents composants des systèmes d'information de l'établissement (réseaux, serveurs, postes de travail, applications…) :

- les audits internes seront effectués sous la responsabilité du RSSI,
- les audits externes seront supervisés par le RSSI, après accord du Président de l'Université d'AixMarseille (en tant qu'AQSSI) pour leur mise en œuvre.

La conformité à la PSSIE et à la PSSI ministérielle sera vérifiée par des contrôles réguliers.

B - Gestion de la SSI

La gestion de la sécurité des systèmes d'information fait l'objet d'un suivi, placé sous la responsabilité du RSSI, permettant d'évaluer, voire de mesurer, les niveaux de sécurité des différents composants de ces systèmes (réseaux, serveurs, postes de travail, applications…).

Pour ce faire, des indicateurs pertinents, choisis suite à des audits des systèmes d'information de l'établissement, permettront de constituer un tableau de bord de la SSI, actualisé avec une périodicité définie.

C - Avis de sécurité sur des matériels ou logiciels

La chaîne fonctionnelle SSI interministérielle (HFDS, FSSI…), ainsi que l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), émettent régulièrement des recommandations quant à l'utilisation de certains matériels ou logiciels dont la mise en œuvre peut s'avérer préjudiciable à la sécurité des systèmes d'information de l'établissement. Les avis émis, peuvent être du niveau « mise en garde » ou du niveau « interdiction » d'utilisation.

XII - Conservation de données, journaux et traces

A - Journalisation des accès et actions sur les systèmes d'information

Les accès aux systèmes d'information de l'établissement doivent être enregistrés dans des fichiers informatiques.

Ces journaux doivent être regroupés sur un serveur dédié, sécurisé dans un VLAN particulier. Ce serveur, qui les centralise et assure leur protection vis-à-vis de l'ensemble des utilisateurs et services de l'établissement, doit être redondé sur un autre serveur, également sécurisé.

La constitution de ces journaux d'accès aux systèmes d'information, présente plusieurs objectifs :

• détecter les actions indues : utilisations non-autorisées, voire frauduleuses, les intrusions,

- en cas d'actions indues :
    - déterminer l'origine de ces actions, les causes techniques qui les ont permises, la nature de ces actions (définir quelle machine a effectué quelles actions, à quelle heure et sur quels composants des systèmes d'information),
    - stopper ces actions indues,
    - apporter les informations techniques demandées par requêtes judiciaires,
- éviter la propagation de programmes indésirables ou d'accès indus, ainsi que les détournements de l'utilisation des ressources informatiques de l'établissement (rebonds systèmes, serveurs pirates, chaînes d'ordinateurs zombies…)
- rétablir les systèmes d'information de l'établissement ou certains de ses composants modifiés indûment ou corrompus au sens des critères de sécurité (Disponibilité, Intégrité, Confidentialité, Traçabilité).

Ces journaux informatiques pourront être transmis aux autorités compétentes, sur requête judiciaire, conformément à la législation française, après avis du Président de l'Université d'Aix-Marseille (en tant qu'AQSSI).

Il est à souligner que la conformité aux lois et règlements en vigueur, s'impose sur les aspects suivants :

- la durée de conservation de ces journaux,
- le respect du « principe de proportionnalité » entre les moyens mis en œuvre et les objectifs visés,
- les contraintes législatives et réglementaires concernant le traitement des informations à caractère personnel,
- l'information des utilisateurs sur la nature des informations collectées, la durée de leur conservation, les buts et la nature des traitements effectués.

B - Traitement des journaux

Les fichiers journaux contenant des informations relatives aux accès aux systèmes d'information de l'établissement, feront l'objet de traitements systématiques et automatisés, afin d'identifier les incidents potentiels ou les événements informatiques pouvant indiquer la survenue de tels problèmes.

Les fichiers journaux contenant des informations relatives aux indicateurs de sécurité des systèmes d'information (ex. nombre de machines dont l'antivirus est à jour), feront également l'objet d'un traitement systématique afin d'évaluer, voire de mesurer, les niveaux de sécurité des différents

composants des systèmes d’information de l’établissement. Ils permettront la constitution et la mise à jour d’un tableau de bord de la sécurité des systèmes d’information de l’établissement.

XIII - Incidents de sécurité

A - Niveaux de sécurité Vigipirate et participation aux exercices PIRANET

Le niveau de sécurité des systèmes d'information de l'université d'Aix-Marseille, est transmis par le Haut Fonctionnaire de Défense et de Sécurité (HFDS) et son Adjoint en charge de l'Education Nationale, au Fonctionnaire de Sécurité et de Défense de l'université. Ce niveau de sécurité correspond aux niveaux « Jaune » et « Orange » du plan Vigipirate.

L'université doit être en capacité de passer en niveau « Rouge » du plan Vigipirate, par la mise en place de procédures et de processus permettant à l'établissement d'avoir la rapidité de réaction nécessaire pour faire face à ce type de situation critique.

L'université sera amenée à participer aux exercices confidentiels du plan d'intervention gouvernemental PIRANET, dont l'objectif est de tester la rapidité et l'efficacité de réaction de la chaîne interministérielle SSI, ainsi que la mise en œuvre des procédures et contre-mesures SSI, dans les établissements concernés.

N.B.1 Les chaînes opérationnelles des ministères concourent à l'effort national de cybersécurité. Les alertes et les incidents sont gérés selon des procédures testées lors d'exercices. La coordination des compétences est organisée à l'échelon ministériel. Les situations d'urgences peuvent faire appel à des mesures définies préalablement dans le cadre des plans gouvernementaux.

N.B.2 En cas d'alerte de sécurité identifiée au niveau national, les RSSI de chaque entité s'assurent de la bonne application des exigences formulées par les instances nationales, dans les meilleurs délais.

B - Gestion d'incidents

Tout incident touchant les systèmes d'information (accès indu, utilisation abusive, vol de données, vol de supports informatiques…) doit être signalé à la chaîne fonctionnelle SSI, au RSSI, ainsi qu'aux autorités hiérarchiques de l'agent et cela systématiquement.

En cas d'implication d'un supérieur hiérarchique dans un incident touchant les systèmes d'information, l'agent contactera directement le RSSI de l'établissement.

En cas d'incident portant potentiellement ou de façon avérée, préjudice au bon fonctionnement d'une entité de l'université d'Aix-Marseille, le RSSI de l'établissement doit en être informé. Le Président de l'Université d'Aix-Marseille (en tant qu'AQSSI) pourra également en être informé en fonction du degré de gravité de l'incident.

Tout incident pouvant induire des suites juridiques pourra faire l'objet d'un dépôt de plainte par l'établissement auprès des autorités compétentes, après avis du Président de l'Université d'AixMarseille (en tant qu'AQSSI).

Lorsqu'un incident se produit dans une entité sous plusieurs tutelles (ex. unités mixtes de recherche), toutes les tutelles devront en être informées. Une concertation entre ces tutelles pourra avoir lieu afin de déterminer quelles suites juridiques devront être données à cet incident.

Les données concernant les incidents feront l'objet d'un traitement informatisé, qui permettra de les intégrer sous forme d'indicateurs, dans le tableau de bord de la SSI de l'établissement.

La remontée d'incidents par les chaînes opérationnelles ministérielles 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'entité ou du ministère, et pour les incidents correspondant à des signalements spécifiques, notamment de la part de l'ANSSI.

C - Gestion de crise

Toute situation de crise potentielle ou avérée, pouvant affecter les systèmes d'information de l'université, doit être signalée au FSD de l'établissement, ainsi qu'au RSSI.

La gestion de crise en cas d'incident, notamment informatique, implique la définition d'une structure (la cellule de crise) propre à répondre à ce type de situation.

Cette structure doit être organisée et mise en place par le Fonctionnaire de Sécurité et de Défense (FSD) de l'établissement.

Concernant l'informatique, elle doit permettre de faire face :

- aux risques liés aux matériels et logiciels informatiques,
- aux risques pouvant affecter les systèmes d'information de l'établissement.

Un outil de Gestion Electronique des Documents (GED) permettra l'organisation des connaissances pour les rendre accessibles en cas de crise et de besoin de partage.

En cas de situation de crise, le FSD informe les structures concernées au sein de l'établissement, voire partenaires de l'établissement, ainsi que le RSSI, le Président de l'Université d'Aix-Marseille (en tant qu'AQSSI), les services du HFDS avec qui il est en relation directe, ainsi que toute autre entité pour laquelle cela s'avérerait nécessaire.

D - Plan de continuité d'activité (PCA)

L'établissement doit se doter d'un plan de continuité d'activité (PCA), destiné au maintien opérationnel des fonctions critiques de ses systèmes d'information de gestion, en cas d'incidents ou de crise informatique. Ainsi, l'université définit la structure et les attendus du plan de continuité d'activité des systèmes d'information de gestion permettant d'assurer effectivement, en cas de sinistre, la continuité d'activité.

Dans un premier temps, ce maintien s'effectue en mode dégradé concernant les performances des systèmes d'information de gestion et permet d'assurer le fonctionnement minimal de l'établissement.

Parallèlement à ce mode opérationnel dégradé, des procédures prévues à cet effet permettent progressivement le rétablissement opérationnel des composants touchés par les incidents informatiques.

Dans un second temps, l'ensemble des systèmes d'information de gestion de l'établissement est rétabli.

Dans les entités relevant de plusieurs tutelles, le PCA doit être construit en concertation.

Le RSSI assure le maintien à jour du plan local de continuité d'activité des Systèmes d'Information de gestion de l'établissement.

Des exercices réguliers sont mis en place afin de tester le plan de continuité d'activité des systèmes d'information de gestion de l'établissement.

Le RSSI s'assure de la bonne mise en œuvre des dispositions prévues dans le plan de continuité d'activité des systèmes d'information de gestion de l'établissement.

Les équipes informatiques mettent en œuvre les dispositifs techniques et les procédures opérationnelles contribuant à la continuité des systèmes d'information de gestion de l'établissement, en assurent la supervision au quotidien et la maintenance dans le temps.

E - Plan de reprise d'activité (PRA)

L'établissement doit se doter d'un plan de reprise d'activité (PRA), destiné à la restauration de ses systèmes d'information de gestion, en cas d'incidents ou de crise informatique qui les auraient arrêtés.

Ce PRA nécessite la mise en place de procédures décrivant les différentes étapes techniques, ainsi que l'existence de moyens informatiques fonctionnels et dissociés des systèmes d'information de gestion de l'établissement, afin de pouvoir les utiliser indépendamment.

Les matériels réseaux font partie de ce PRA.