UNIVERSITÉ DE TOULON

Direction du Système d'Information et des Usages Numériques

Politique de Sécurité du Système d'Information

PSSI de l'université de Toulon

10/01/2020

Préambule

La politique de sécurité du système d'information de l'université (PSSI) définit un cadre pour la gestion de la sécurité du système d'information.

Elle énonce les règles organisationnelles et techniques à mettre en œuvre pour assurer la sécurité du système d'information.

Elle s'appuie sur la politique de sécurité des systèmes d'information de l'Etat (PSSIE).

La PSSI s'adresse à l'ensemble des utilisateurs du système d'information de l'établissement.

Le présent document est le résultat d'un groupe de travail constitué des membres suivants :

- Le directeur général des services (DGS).
- Le vice-président conseil d'administration.
- Le vice-président délégué au numérique (ou porteurs politiques identifiés sur ces domaines).
- Le directeur du système d'information (DSI) et son adjoint.
- Le responsable de la sécurité du système d'information (RSSI) et son adjoint.
- Le fonctionnaire sécurité défense (FSD) et son adjoint.
- Le délégué à la protection des données (DPD).
- Le référent prévention radicalisation.
- Le responsable du pôle moyen informatique de la direction du système d'information et des usages numériques (DSIUN).
- Le responsable du service audiovisuel et informatique de l'iut (SA2I) ou son représentant.
- Le directeur des ressources humaines (DRH) ou son représentant.

1 Politique, organisation, gouvernance

1.1 Organisation de la Sécurité du Système d'Information (SSI)

1.1.1 Le comité de pilotage SSI

Sous l'autorité du président de l'université, le comité de pilotage SSI se réunit au minimum une fois par an en fin d'année universitaire.

Il est composé des membres suivants :

- Le président de l'université.
- Le vice-président délégué aux ressources humaines et au dialogue social (ou porteurs politiques identifiés sur ces domaines).
- Le vice-président du conseil d'administration.
- Le fonctionnaire de sécurité de défense (FSD) et son adjoint.
- Les membres du comité de pilotage SSI restreint.

Des personnalités qualifiées pourront être invitées suivant l'ordre du jour.

Le comité de pilotage SSI :

- Définit les axes stratégiques en matière de SSI, valide les plans d'actions, réalise les arbitrages budgétaires et organisationnels ;
- Examine les bilans des incidents et audits de sécurité transmis par le comité de pilotage SSI restreint et valide la mise en œuvre des mesures préconisées par celui-ci ;
- Assure le suivi de la SSI à l'aide des tableaux de bord fournis par le comité de pilotage SSI restreint ;
- Valide les éventuelles mises à jour de la PSSI proposées par le comité PSSI restreint.

1.1.2 Le comité de pilotage SSI restreint

Le comité de pilotage SSI restreint se réunit au minimum trois fois par an à l'initiative du RSSI, et peut être réuni en cas d'incident grave de sécurité pour prise de décision.

Il est composé des membres suivants :

- Le vice-président délégué au numérique (ou porteurs politiques identifiés sur ces domaines).
- Le directeur général des services (DGS).
- Le directeur du système d'information (DSI) et son adjoint.
- Le responsable de la sécurité du système d'information (RSSI) et son adjoint.
- Le délégué à la protection des données (DPD).

Des personnalités qualifiées pourront être invitées suivant l'ordre du jour.

Le comité de pilotage SSI restreint :

- Coordonne les activités liées à la SSI, relaye les décisions au comité de pilotage et lui fournit les informations nécessaires sur l'état des lieux de la SSI ;
- Pilote et suit la mise en œuvre des plans d'actions nécessaires à la mise en œuvre de la PSSI à l'aide d'indicateurs d'avancement permettant de mesurer le déploiement des mesures de sécurité retenues par la PSSI ;
- Suit l'efficience des mesures déployées grâce aux indicateurs de celles-ci ;
- Réalise les tableaux de bord pour le comité de pilotage ;
- Assure le suivi des incidents de sécurité à l'aide d'indicateurs remontés par le RSSI et de la synthèse des incidents survenus depuis la dernière séance du comité et en dresse un bilan ;
- Examine les rapports d'audit que peut être amené à faire le RSSI, préconise l'adaptation des mesures de sécurité existantes ou de nouvelles mesures de sécurité et expose ses conclusions au comité de pilotage.

1.1.3 Rôles et responsabilités des acteurs SSI

1.1.3.1 L'Autorité Qualifiée pour la Sécurité du Système d'Information (AQSSI)

Le président de l'université, assure la responsabilité globale de la sécurité du système d'information de l'établissement, il peut être juridiquement responsable en cas d'incident de sécurité.

L'AQSSI :

- Préside le comité de pilotage SSI ;
- S'appuie sur le RSSI, chargé de l'assister dans le pilotage et la gestion de la SSI ;
- Veille à la mise en œuvre des dispositions contractuelles et réglementaires sur la sécurité du SI, s'assure que les contrôles internes de sécurité sont régulièrement effectués et fait organiser la sensibilisation et la formation du personnel aux questions de sécurité ;
- Propose au conseil d'administration la Politique de Sécurité du Système d'Information et les mesures de sécurité retenues par celle-ci ;
- Accorde les moyens budgétaires, humains, techniques pour mettre en application les directives de celle-ci ;
- S'implique dans les décisions de management, et soutient la démarche engagée.

1.1.3.2 Le Fonctionnaire de Sécurité de Défense et son adjoint (FSD)

Nommé par le Haut Fonctionnaire de Défense et Sécurité (HFDS) du ministère, il est son relais fonctionnel au sein de l'établissement.

Le FSD :

- A un rôle de coordination, de conseil, d'information et de mise en œuvre dans le cadre de la protection du potentiel scientifique et technique (PPST), de la protection du secret et de la préparation / exécution des plans de défense et de sécurité ;
- Participe à l'identification, à l'évaluation et au traitement des risques ;

1.1.3.3 Le Directeur du Système d'Information et son adjoint (DSI)

Le DSI :

- Met en œuvre la PSSI et fait appliquer les règles de sécurité dans son périmètre ;
- Maintient et garantit la disponibilité et le bon fonctionnement des moyens et ressources informatiques ;
- Participe activement à la veille sécuritaire et technologique ;
- Fait vérifier régulièrement la vulnérabilité des infrastructures techniques en collaboration avec le RSSI et l'informe systématiquement des travaux susceptibles d'impacter les dispositifs de sécurité en place ou d'influencer la cartographie des risques.

1.1.3.4 Le Responsable de la Sécurité du Système d'Information et son adjoint (RSSI)

Désigné par l'AQSSI, dont il dépend fonctionnellement en matière de SSI, il veille à la sécurité des données et informations de l'établissement en termes de confidentialité, intégrité, disponibilité et traçabilité.

Le RSSI doit être formé à la SSI, cette fonction doit être assumée par un agent titulaire et non pas par un prestataire.

Le RSSI :

- S'assure de l'identification, de l'évaluation et du traitement des risques relatifs au système d'information ;
- Pilote les actions de sensibilisation et de formation du personnel de l'établissement ;
- Participe à la veille technique et juridique ;

- Assure la coordination avec les organismes concernés par la SSI ;
- Coordonne et vérifie, en appui avec la Direction des Affaires Juridiques, l'intégration et le respect des clauses de sécurité dans tout contrat ou convention impliquant un accès au SI par des tiers ;
- Assure la gestion des incidents SSI et maintient à jour les indicateurs et le suivi des incidents ;
- Pilote en collaboration avec le DSI, la mise en œuvre opérationnelle de la sécurité et organise régulièrement des audits de sécurité ;
- Est responsable de l'élaboration de la PSSI, de sa mise à jour, du contrôle et du suivi de l'application des mesures de celle-ci ;
- Élabore et assure le suivi des plans d'action nécessaires à la mise en œuvre de la PSSI ;
- Diffuse à l'ensemble de la communauté universitaire les documents relatifs à la PSSI et son application ;
- Définit et maintient les indicateurs et tableaux de bord SSI à destination des comités de pilotage.

1.1.3.5 Le délégué à la protection des données (DPD)

Conformément au règlement européen sur la protection des données (RGPD), il est nommé par le président.

Le DPD a pour mission :

- D'informer et conseiller le responsable de traitement (le président de l'université), ainsi que les personnels qui procèdent au traitement, sur les obligations qui leur incombent en matière de protection des données à caractère personnel ;
- D'auditer et contrôler le respect du RGPD et du droit national en matière de protection des données ;
- De veiller à l'application du principe de protection des données dès la conception et par défaut dans tous les projets comportant un traitement de données personnelles ;
- D'être l'interlocuteur privilégié de l'autorité de contrôle (CNIL) et coopérer avec elle ;
- De dispenser des conseils en ce qui concerne les analyses d'impact relatives à la protection des données et d'en vérifier l'exécution ;
- De tenir l'inventaire et documenter les traitements de données à caractère personnel en tenant compte du risque associé à chacun d'entre eux compte tenu de sa nature, sa portée, du contexte et de sa finalité ;
- De rendre compte de ses activités au responsable de traitement.

1.1.3.6 Les directeurs de composantes et directions

Les directeurs des composantes et directions sont garants dans leur domaine de l'application des règles de sécurité de la PSSI.

Ils :

- S'assurent que les personnels de leur direction respectent les bonnes pratiques et la charte de bon usage du système d'information ;
- Veillent à ce que tout nouveau projet fasse l'objet d'une étude formalisant les besoins, risques et objectifs de sécurité ;

- Valident les demandes de droit d'accès à une application de leur périmètre et s'assurent de leur mise à jour en cas de mouvement du personnel, ils s'engagent à réaliser une revue annuelle de ces droits ;
- Remontent au RSSI les procédures déjà en place, les besoins de sécurité et les incidents et vulnérabilités décelés pouvant porter atteinte à la sécurité des informations. L'analyse des incidents de sécurité menée par le RSSI sera, selon le degré de gravité de l'incident, transmise au DPD.

1.1.3.7 La Direction des Ressources Humaines

La direction des ressources humaines, effectue l'ensemble des démarches nécessaires à l'accompagnement de nouvelles mesures de sécurité, dans le cadre des plans d'actions arrêtés par le comité de pilotage SSI. Elle veille notamment à l'intégration de sessions de formation à la sécurité du système d'information dans le plan de formation du personnel dont le cahier des charges aura été préalablement défini par le RSSI.

1.1.3.8 La Direction des Affaires Juridiques et Institutionnelles

La direction des affaires juridiques et institutionnelles s'assure que les mesures de la politique de sécurité sont conformes aux exigences réglementaires et doit être particulièrement vigilante afin d'inclure les clauses de sécurité dans les documents, contrats, conventions, etc., impliquant un accès au SI par des tiers.

1.1.3.9 Les administrateurs du SI

Les administrateurs du SI assurent des missions de conception, d'exploitation et de maintien en condition opérationnelle des ressources informatiques. Ils possèdent à ce titre des accès étendus aux ressources informatiques. Ces accès doivent être utilisés dans un cadre légal et respectueux des utilisateurs et de la déontologie.

Ils :

- Participent activement à la protection du système d'information ;
- Veillent à sécuriser les ressources qu'ils administrent ;
- Suivent les règles de sécurité de la PSSI ;
- Informent le RSSI des incidents de sécurité dont ils seraient témoins ;
- Participent à la sensibilisation des utilisateurs à la sécurité du SI .

1.1.3.10 Les directeurs de laboratoires

Les directeurs de laboratoires sont les garants de la protection des données scientifiques et industrielles sensibles de leur laboratoire. Ils veillent à faire appliquer les règles de sécurité de la PSSI, et s'assurent que les personnels de leur laboratoire respectent les bonnes pratiques et la charte de bon usage du système d'information.

Ils sont le contact privilégié du RSSI pour leur laboratoire et lui remontent les procédures déjà en place, les besoins de sécurité, les incidents et vulnérabilités décelés pouvant porter atteinte à la sécurité du système d'information.

Dans le cas des laboratoires en cotutelle, si un correspondant sécurité est nommé, il est alors le contact privilégié du RSSI, le directeur du laboratoire communique ses coordonnées au RSSI.

Dans le cas où les tutelles auraient elles aussi une PSSI, un examen de celle-ci doit être fait en collaboration avec le comité de pilotage SSI restreint afin d'harmoniser les mesures préconisées par les différentes tutelles.

Dans le cas particulier des laboratoires en Zone à Régime Restrictif (ZRR), des mesures de sécurité plus spécifiques doivent être mises en œuvre et font l'objet d'une politique spécifique.

1.1.3.11 Les utilisateurs du système d'information

Toute personne ayant un accès au système d'information de l'établissement est responsable du respect des règles de sécurité des outils mis à sa disposition et des données qu'elle manipule.

Elle se doit de se conformer à la charte du bon usage du système d'information de l'établissement et d'informer le RSSI des incidents de sécurité dont elle serait témoin (vol de document, vol de poste de travail, divulgation de données à caractère personnel, usurpation d'identité, etc.).

1.2 Définition et pilotage de la Politique de Sécurité du Système d'Information

1.2.1 Gestion du document « Politique de Sécurité du Système d'Information »

Sous la responsabilité du comité de pilotage SSI restreint, la PSSI est revue annuellement, et chaque fois qu'un changement majeur dans le contexte de l'établissement l'imposerait (évolution du système d'information, des besoins de sécurité et des risques identifiés).

La version modifiée est soumise pour approbation au comité de pilotage SSI, le conseil d'administration de l'établissement valide la version finalisée du document après avis du Comité Technique d'Etablissement Public (CTEP).

1.2.2 Application de la Politique de Sécurité du Système d'Information

Le RSSI élabore les plans d'action nécessaires à la mise en œuvre de la PSSI, les comités de pilotage SSI les valident et les priorisent.

Le RSSI assure la coordination de la mise en œuvre des plans d'action et rend compte régulièrement aux comités de pilotage SSI.

Le déploiement des mesures de sécurité est suivi au travers d'indicateurs d'avancement et d'indicateurs de conformité à la politique de sécurité des systèmes d'information de l'état (PSSIE). Ces indicateurs sont ensuite agrégés en tableaux de bord SSI.

1.2.3 Contrôle et suivi

Chaque mesure de sécurité déployée fait l'objet d'au moins un indicateur d'efficacité, qui doit être défini dans le document de mise en œuvre de celle-ci.

Ces indicateurs sont suivis par le comité de pilotage SSI restreint lors de chacune de ses réunions et sont agrégés en tableaux de bord fournis au comité de pilotage SSI.

Des tests et audits techniques sont menés sous la responsabilité du RSSI et du DSI, afin de contrôler le bon fonctionnement des mesures de sécurité déployées. Les rapports d'audit sont transmis aux comités de pilotage SSI pour analyse et prise de décisions.

2 Sécurité liée aux ressources humaines

2.1 Responsabilité des utilisateurs

Les droits, devoirs et responsabilités qui incombent à tout utilisateur du SI en matière de sécurité, sont précisés dans la charte de bon usage du système d'information.

Deux versions de cette charte sont disponibles : l'une à destination des étudiants, l'autre à destination des autres usagers (personnels, stagiaires, prestataires, etc).

La charte est annexée au règlement intérieur de l'établissement et communiquée à tout utilisateur lors de sa première connexion à un service numérique.

2.2 Postes clés de la SSI, et postes dits de confiance

Les personnes occupant les postes clés de la SSI (RSSI, administrateurs des SI, correspondants SSI, etc.) ainsi que les postes dits de confiance (manipulant des informations sensibles) doivent être régulièrement sensibilisés aux devoirs liés à leur fonction.

L'aptitude à respecter les règles de sécurité doit être prise en considération lors du recrutement du personnel. La fiche de poste doit également préciser la sensibilité SSI, les risques SSI et la protection du patrimoine et potentiel scientifique et technique liés à ces postes :

- Biens sensibles concernés et mesures spécifiques ;
- Activités sensibles et règles à suivre ;
- Engagement de confidentialité sur les informations accédées.

2.3 Gestion des tiers

Tout accès d'un tiers au SI de l'établissement doit faire l'objet d'une demande explicite auprès du DSI ou de son représentant qui pourra consulter le RSSI. Cette demande doit spécifier les besoins, permettre d'identifier les risques afin de définir les mesures de sécurité complémentaires à mettre en œuvre.

Toute structure (direction, composante, laboratoire, etc.) souhaitant pour des raisons d'installation/maintenance permettre à un tiers l'accès à un serveur, un poste de travail ou une application du SI doit en faire la demande au minimum une semaine à l'avance.

Cet accès est nominatif, pour un ensemble de serveurs / poste de travail donné, et se fait au travers de la passerelle d'accès sécurisé (VPN) de l'université. Une dérogation pour un outil tiers est éventuellement possible de façon temporaire et sous conditions.

Une clause de confidentialité est annexée dans les contrats signés avec les tiers dès lors que la prestation nécessite un accès au SI et/ou à des informations sensibles.

Les intervenants signent la charte de bon usage du SI de l'établissement et s'engagent à ne pas divulguer les informations dont ils auraient pu prendre connaissance.

2.4 Formation et sensibilisation

Il est important que chaque personne soit sensibilisée aux enjeux de la sécurité et soit formée de manière à pouvoir gérer les mesures de sécurité qui lui incombent.

Pour cela le plan de formation de l'établissement prévoit plusieurs types de formations :

- Une formation en présentiel ou en ligne obligatoire devra être suivie par les personnels a minima tous les deux ans ;
- Une formation spécifique pour les personnels assurant les postes clés de la SSI ;
- Une formation spécifique pour les personnels manipulant des données sensibles ;
- Une formation spécifique pour les personnels de direction.

Parallèlement aux sessions de formation, chaque utilisateur a accès à un ensemble de support de sensibilisation, diffusés via le site web de l'établissement, les écrans d'information situés dans les halls des bâtiments, des affichettes, etc.

2.5 Mouvement de personnel et gestion des habilitations

Des procédures relatives aux arrivées, mutations et départs des personnes sont élaborées en collaboration par les directions concernées (DRH, DEVE, DSIUN, DPST, DAS, …).

Ces procédures définissent a minima les principes de la gestion du cycle de vie des comptes numériques, des droits d'accès aux ressources du système d'information, du contrôle d'accès aux locaux, des équipements mobiles.

Elles sont diffusées aux utilisateurs par différents canaux et sont appliquées strictement.

Toute demande de dérogation doit faire l'objet d'une étude par le comité de pilotage SSI restreint et validée par le président de l'université.

En cas de mouvement d'un personnel d'un poste à un autre, celui-ci perd automatiquement, à la date de sa nouvelle affectation, les droits d'accès aux applications métier que le poste qu'il occupait nécessitaient. Sauf demande formelle du directeur de la structure de départ, sur un temps limité et sous réserve d'accord du DGS ou de son représentant.

Les habilitations d'accès sont revues a minima une fois par an.

Il est de la responsabilité des responsables fonctionnels d'une application (par défaut le directeur de la structure en charge du support fonctionnel de l'application) de contrôler la légitimité des habilitations d'accès à celle-ci. Pour ce faire la DSIUN leur fournira annuellement un état des lieux des habilitations. Un compte rendu des opérations effectuées (retrait, ajout, maintien, etc…) sera envoyé au comité de pilotage SSI restreint.

3 Gestion des biens

3.1 Inventaire des ressources informatiques et cartographie

L'ensemble des ressources informatiques (applications, serveurs, équipements réseau, postes de travail, smartphones, imprimantes, téléphones Ip et de façon générale tout équipement sous la responsabilité de l'établissement) fait l'objet d'un inventaire, accessible aux RSSI, DSI et aux

responsables de structure pour le parc qui les concernent. Chaque nouveau projet ou acquisition entraîne l'inventaire des ressources associées.

La mise à jour de l'inventaire est contrôlée périodiquement a minima une fois par an.

3.2 Qualification et protection de l'information

L'utilisateur est responsable de l'usage et de la protection de l'information qu'il manipule tout au long de son cycle de vie, de sa création à sa destruction.

L'établissement définit une échelle permettant aux utilisateurs d'évaluer le niveau de sensibilité / confidentialité de l'information qu'ils manipulent. Les règles de protection de l'information (marquage des documents, chiffrement, signalement aux DPD et RSSI, etc.) sont définies et adaptées selon le niveau de celle-ci.

4 Intégration de la SSI dans le cycle de vie du système d'information

La sécurité est prise en compte à toutes les étapes d'un projet lié au système d'information, et ce, jusqu'à son terme : phase d'expression des besoins, rédaction du cahier des charges, conception, exploitation, etc.

Les applications liées à la recherche et à la pédagogie déployées par les laboratoires et composantes le sont sous leur entière responsabilité.

Il appartient à la personne responsable du déploiement d'une telle application d'analyser la criticité des données traitées et de mettre en œuvre les mesures de sécurité adéquates.

La personne responsable de l'application doit se rapprocher des services compétents (DAJI, DPD, DSIUN), si cette application implique un ou des traitements de données personnelles, ou, plus généralement, si la mise en œuvre de l'application peut représenter un risque pour la sécurité du SI de l'établissement.

Les services support (DGS, DAJI, DSIUN, DIREP) peuvent être consultés pour apporter leurs expertises ou celles des réseaux partenaires (ANSSI, RENATER, CNIL, réseau des RSSI, réseau des DPD, …) afin de réaliser l'analyse des risques.

Les applications métier de l'établissement sont déployées et maintenues sous la responsabilité technique de la DSIUN. Celle-ci doit être associée à tous projets de déploiement de telles applications par les directions métier. Elle émettra un avis sur l'adéquation de l'outil par rapport aux besoins exprimés ainsi que sur son impact sur le SI (notamment sécurité).

Il est de la responsabilité de la DSIUN de veiller au maintien de la cohérence du SI et de sa sécurité pour l'ensemble des applications métier, que celles-ci soient en mode hébergé ou en mode service.

4.1 Entrée dans le système d'information

Toute nouvelle brique du SI sous la responsabilité de la DSIUN, fait l'objet d'une déclaration formelle de mise en production validée par le DSI.

Celle-ci a pour but de s'assurer :

- Du respect des règles de sécurité et de développement préconisées ;
- De la validation du bon fonctionnement de l'application ou du matériel par une phase de recette ;
- De la correction des vulnérabilités découvertes par les éventuels tests réalisés (analyse de code, test d'intrusion, recherche de vulnérabilités, etc.) ;
- De l'ajout de l'application ou du matériel à la cartographie du SI ;
- De la déclaration du traitement auprès du DPD et de la réalisation d'une analyse d'impact sur la protection des données si besoin ;
- De l'estimation du niveau de sécurité requis en termes de disponibilité, intégrité et confidentialité ;
- De la sécurisation de l'environnement de l'application ou du matériel (plan de mise à jour, supervision, sauvegarde, documentation d'exploitation, etc.).

Il incombe au responsable du déploiement de l'application ou du matériel au sein du SI, de constituer et de transmettre au DSI, le dossier permettant cette analyse.

4.2 Maintien en condition opérationnelle et gestion des changements

Toute évolution majeure d'une brique du SI, sous la responsabilité de la DSIUN (changement de matériel, mise à jour, modification de configuration, etc.), fait systématiquement l'objet d'un processus de recette formalisé par un plan de test défini avant la mise en production initiale de celle-ci.

Ce processus de recette est réalisé dans un environnement dédié de pré-production avant son application dans l'environnement de production.

Les opérations de maintenance sont documentées, planifiées et annoncées aux usagers, au minimum, une semaine en avance.

En cas de mise en œuvre de changement en urgence, en cas de découverte de vulnérabilités par exemple, des mesures de contrôle du bon fonctionnement des modifications effectuées et de l'absence d'effet de bord doivent être prévues et appliquées.

4.3 Sortie du système d'information

Lorsqu'une brique du SI, sous la responsabilité de la DSIUN est remplacée par une autre ou qu'elle n'est plus nécessaire au bon fonctionnement du SI, le retrait de celle-ci doit être planifié et porté à la connaissance du DSI ou de son représentant.

La personne en charge du retrait, s'assure notamment de la mise à jour de la cartographie du SI et de la suppression sécurisée des données.

4.4 Produits et services labellisés

Lorsqu'ils sont disponibles, les produits ou services de sécurité labellisés (certifiés, qualifiés) par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) doivent être utilisés.

4.5 Gestion des prestataires

Tout recours à des prestataires extérieurs doit être porté à la connaissance du DSI ou de son représentant.

Des clauses de sécurité issues d'une rapide analyse de risque, doivent être intégrées au cahier des charges de tout projet relatif au SI.

Dans le cadre d'un hébergement externalisé, le contrat détaille les mesures prises pour assurer la sécurité des données, et la réversibilité de celles-ci. Dès lors qu'il s'agit de données personnelles, l'hébergement est limité à des entreprises de droit européen, sauf dérogation du FSD.

Une clause de confidentialité est annexée dans les contrats signés avec les tiers, dès lors que la prestation nécessite un accès au SI et/ou à des informations sensibles.

Lorsqu'il s'avère qu'un prestataire sous-traite les données de l'université (hébergement ou maintenance d'un service informatique, intégrateur de logiciel et plus généralement, tout organisme offrant une prestation impliquant un traitement de données pour le compte de l'université, …), le prestataire doit présenter des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées. Un contrat ou autre acte juridique est alors signé entre l'université et le sous-traitant (prestataire) et contient les dispositions de l'article 28 du RGPD. Le DPD est préalablement consulté pour l'élaboration du contrat.

Les intervenants signent la charte de bon usage du SI de l'établissement et s'engagent à ne pas divulguer les informations dont ils auraient pu prendre connaissance.

5 Sécurité physique

5.1 Définition des périmètres de sécurité physique

Les différents sites de l'université sont découpés en zones de sécurité de niveaux différents, chaque zone possède sa propre politique d'accès. Le découpage en zone et l'élaboration de la politique d'accès est réalisé conjointement par la Direction du Patrimoine et des Services Techniques (DPST), les responsables des zones, le comité de pilotage SSI restreint et le cas échéant le FSD et/ou son adjoint.

Le niveau et la politique d'accès de chaque zone est porté à la connaissance des personnels localisés dans celle-ci pour leur bonne application.

5.2 Contrôle des accès physiques, gestion des autorisations

Des procédures relatives à l'attribution, révocation des habilitations d'accès aux locaux et à la délivrance, restitution des cartes, badges, clés, etc. sont élaborées par la DPST et validées par les comités de pilotage SSI.

Les habilitations d'accès aux locaux sont revues a minima une fois par an et font l'objet d'un rapport remis au comité de pilotage SSI restreint.

La gestion des affectations des locaux relève exclusivement de la DPST. Toute personne souhaitant changer la destination d'un local (changement d'usage du local, changement de bureau) doit suivre la procédure adéquate et impérativement informer la DPST avant toute prise de décision.

5.3 Sécurité physique des salles serveurs et locaux techniques

Dans le cas où les locaux seraient mutualisés entre plusieurs entités, un découpage en zone de sécurité différentes est à réaliser.

Dans le cadre d'hébergement de tiers, une convention de service définissant les responsabilités des différentes parties doit être établie.

Les locaux (ainsi que les différentes zones des locaux) bénéficient d'un contrôle d'accès permettant une traçabilité et d'une procédure de surveillance adaptée. Les locaux les plus sensibles doivent disposer d'un système d'alarme et de vidéoprotection.

Les accès physiques de ces locaux sont sécurisés notamment en minimisant les ouvertures sur l'extérieur, en les équipant de barreaux, grilles, volets, etc.

Les locaux disposent des équipements d'infrastructure (climatisation, équipement de protection incendie, alimentation électrique, …) correctement dimensionnés, adaptés à la spécificité de l'usage qu'il en est fait (notamment datacenter) et présentant dans la mesure du possible une redondance suffisante. Ces équipements sont couverts par des contrats de maintenance et si nécessaire par des contrats de service pour en assurer l'exploitation.

Des procédures de réaction en cas de panne ou d'incident sont formalisées, connues du personnel et vérifiées annuellement.

5.4 Système d'information de sûreté

Le SI de sûreté regroupe :

- Les services support des activités de contrôle d'accès et de détection d'intrusion ;
- Les services support des activités de vidéoprotection ;
- Les services support de la gestion technique des bâtiments ;
- Les services support de la sécurité incendie.

Tous les éléments composant le SI de sûreté doivent faire l'objet de mesures de sécurité spécifiques.

Dans le cas particulier de la vidéoprotection, un système de gestion centralisée est préférable à plusieurs systèmes autonomes. Les procédures de gestion de celui-ci définissant les rôles de chacun sont établies et suivies. La rétention des données est effectuée sur une fenêtre glissante d'un mois et les vidéos sont conservées sur un système isolé dont l'exploitation est restreinte aux seules personnes habilitées.

6 Sécurité des réseaux

6.1 Réseaux nationaux

Des équipements d'infrastructure sont mis en œuvre afin de protéger et d'isoler le réseau interne vis-à-vis de l'extérieur. Des adresses ip non routables et un mécanisme de traduction d'adresses sont ainsi utilisés, protégeant en confidentialité le plan d'adressage interne, classifié comme sensible.

Des mécanismes de filtrage sont mis en œuvre afin d'assainir les flux sortants et entrants, et de limiter les possibilités d'attaques. La DSIUN s'appuie notamment sur le service anti-spam de RENATER pour assainir les flux de messagerie.

Les accès à internet (même pour un site délocalisé tel que Draguignan) passent obligatoirement par les passerelles de sécurité mises en œuvre.

Les informations sensibles transitant sur des réseaux non maitrisés sont spécifiquement protégées par un chiffrement adapté.

6.2 Réseaux locaux

Seules les personnes légitimes, c'est-à-dire enregistrées dans le SI de façon permanente ou temporaire peuvent accéder au réseau de l'établissement et bénéficier des services numériques pour lesquels elles sont habilitées.

L'administration du réseau de l'établissement est sous la responsabilité exclusive de la DSIUN.

Les équipes techniques de la DSIUN, en charge du réseau, mettent en place et exploitent les éléments de sécurité nécessaires (équipements, architecture logique).

Des zones de sécurité sont définies afin de cloisonner le système d'information en zones de niveaux de sécurité et de confiance homogènes. Un filtrage des accès est mis en œuvre entre ces différentes zones.

Les zones sensibles sont isolées par des mesures de sécurité réseau spécifiques.

Par exemple, les différents serveurs de l'établissement sont a minima répartis dans les zones suivantes:

- Serveurs accessibles de l'internet ;
- Serveurs accessibles par les usagers du campus ;
- Serveurs de test et développement ;
- Serveurs d'infrastructure ;
- Serveurs nécessitant une visibilité restreinte (base de données, etc.).

6.2.1 Equipements non maîtrisés

Le déploiement d'équipements réseau (commutateur, borne, vpn, hub, etc.) sur l'ensemble du campus relève exclusivement de la responsabilité de la DSIUN. Il peut être réalisé par les équipes de proximité avec l'accompagnement et la validation techniques de l'équipe réseau de la DSIUN. Ainsi, aucun équipement ne peut être mis sur le réseau de l'établissement sans accord préalable.

Les nouveaux besoins de connexion au réseau nécessitant par exemple l'activation de prise, l'ajout de prise, etc. font l'objet d'une demande formelle. Une réponse est apportée dans les meilleurs délais par l'équipe réseau de la DSIUN. La DSIUN peut déléguer aux services informatiques en composante, la possibilité de connecter et reconnecter physiquement les équipements.

Les équipements réseau sont identifiés et répertoriés et font l'objet d'un document de cartographie.

6.3 Réseaux sans fil

Le déploiement de bornes et réseaux sans fil (WiFi) sur l'ensemble du campus relève exclusivement de la responsabilité de la DSIUN.

A l'instar du réseau filaire, le réseau sans fil est cloisonné par niveaux de sécurité homogènes. Ainsi différents accès au réseau sans fil (WiFi) sont proposés aux usagers, lesquels sont également avertis des risques inhérents à ceux-ci.

L'établissement peut être amené à prendre toutes mesures nécessaires à la préservation de la sécurité du réseau sans fil, notamment la désactivation de toutes bornes pirates qui seraient détectées.

6.4 Accès spécifiques

Les accès spécifiques à internet nécessitant des droits particuliers ne sont possibles que sur dérogation dûment justifiée et font l'objet d'une demande formelle étudiée par les équipes techniques de la DSIUN pour une réponse adaptée.

Tout accès depuis un réseau extérieur sur un serveur ou poste de travail de l'établissement est soumis à autorisation de la DSIUN. Les accès des partenaires et des personnels de l'université se font uniquement au travers de la passerelle d'accès sécurisé (VPN) selon la procédure établie.

6.5 Administration et exploitation

L'administration et la supervision du réseau se font depuis des équipements dédiés situés dans une zone spécifique et isolée.

Le contrôle d'accès logique aux équipements se fait exclusivement via des comptes nominatifs, dont les mots de passe sont régulièrement changés. Les mots de passe constructeur par défaut sont systématiquement modifiés.

Un tableau de bord permettant une vision globale des différents accès sur les équipements réseau est accessible aux DSI et RSSI. Un contrôle régulier des accès et droits alloués est réalisé par l'équipe réseau de la DSIUN. Le DSI et le RSSI sont immédiatement avertis en cas de problème constaté.

Les opérations d'administration et d'exploitation sensibles (par exemple les opérations impactant la configuration des équipements) sont tracées et journalisées au moyen de rapports d'intervention ou d'enregistrement des connexions et actions effectuées par les administrateurs.

Les procédures d'exploitation du réseau sont formalisées, documentées et maintenues à jour. Elles sont disponibles en diffusion restreinte aux personnes habilitées.

6.5.1 Sécurité de l'infrastructure

La configuration des équipements réseau fait l'objet de mesures de durcissement définies et appliquées. Elles concernent a minima la sécurisation des accès aux interfaces d'administration, l'application des mises à jour et correctifs de sécurité, la gestion des comptes et privilèges.

Toutes les prises réseau sont identifiées et localisées et font l'objet d'une cartographie. Une politique concernant le brassage et l'activation des prises réseau est établie et mise en œuvre, conciliant sécurisation de l'accès au réseau et qualité de service aux usagers.

Les accès aux locaux de brassage sont contrôlés et journalisés ; ils font l'objet d'un audit régulier.

Les équipements critiques sont configurés voire redondés pour en assurer la disponibilité.

Les activités réseau font l'objet d'une surveillance permettant de s'assurer de la disponibilité et de la qualité de service du réseau.

Des dispositifs d'audit sont mis en œuvre permettant la journalisation des principaux événements liés à la sécurité des réseaux. Les journaux d'audit sont analysés quotidiennement par l'équipe réseau de la DSIUN afin de détecter d'éventuels incidents de sécurité.

Les journaux d'audit sont classés comme sensibles, ils sont sauvegardés, protégés et conservés pendant une période satisfaisant les exigences légales.

6.6 Cartographie

L'architecture du réseau de l'établissement est décrite et formalisée au travers notamment de schémas décrivant les interconnexions des différents équipements et sous-réseaux, d'inventaires des différents équipements et prises réseau, de plans de câblage, etc.

La cartographie du réseau s'insère dans la cartographie globale du système d'information, elle est actualisée au fil de l'eau par l'équipe réseau de la DSIUN et fait l'objet d'une revue par l'urbaniste de l'établissement au minimum une fois par an.

Les documents de cartographie sont classés comme sensibles et font l'objet d'une protection adaptée. Leur accès est limité aux personnes habilitées.

7 Architecture et Exploitation du système d'information

L'architecture du SI est définie de façon à satisfaire l'ensemble des besoins de l'établissement, en terme de disponibilité, confidentialité, traçabilité et intégrité des données.

7.1 Généralités

L'échange de données, entre les différentes applications, s'effectue uniquement via des protocoles sécurisés.

Les environnements de production, de développement et de pré-production doivent être isolés les uns des autres.

L'infrastructure de stockage et de sauvegarde doit reposer sur une architecture dédiée.

7.2 Sécurité des ressources informatiques

La connaissance de l'environnement numérique est un préalable à la sécurité des ressources informatiques. Il est nécessaire de disposer d'une cartographie à jour des ressources en production et des interventions de maintenance les impactant (ex : mise à jour, changement de configuration, etc.). L'historique des interventions doit être accessible au RSSI sur une période d'au moins un an.

Il peut être nécessaire de documenter des procédures d'exploitation dans le cas de ressource identifiée comme critique par le responsable de celle-ci.

7.3 Gestion des autorisations et contrôle d'accès logique aux ressources

L'accès à toute ressource informatique protégée nécessite identification et authentification individuelle de l'utilisateur.

Les applications manipulant des données particulièrement sensibles doivent permettre une gestion fine des accès des utilisateurs et privilégier une authentification forte.

Le processus d'autorisation d'accès à une ressource informatique est formalisé et s'appuie sur les procédures relatives aux arrivées, mutations et départs des personnes.

Chaque personne se voit attribuer les droits d'accès nécessaires et suffisants à l'exercice de ses missions.

Une revue des autorisations d'accès doit être réalisée annuellement.

7.3.1 Gestion des authentifiants

Les informations d'authentification, comme les mots de passe, sont considérées comme des données sensibles. Elles doivent être conservées de manière sécurisée, et ne doivent être ni stockées, ni transiter en clair sur les réseaux.

Sauf contrainte technique particulière, l'accès aux différentes ressources informatiques de l'établissement doit être basé sur une authentification centralisée utilisant les comptes numériques délivrés par la DSIUN, et automatiquement désactivés, selon le cycle de vie défini par l'établissement.

En cas d'impossibilité, des moyens techniques permettant d'imposer les règles de gestion des mots de passe de l'établissement aux comptes locaux, doivent être mis en œuvre.

Le cycle de vie des comptes locaux doit être formalisé et suivi. En particulier, chaque compte local à une ressource doit être créé avec un mot de passe initial fort respectant les règles de gestion de mots de passe de l'établissement et doit être supprimé au départ de l'utilisateur.

7.3.2 Gestion des authentifiants d'administration

L'administration des postes de travail et serveurs doit se faire en utilisant des comptes d'administration nominatifs et non les comptes d'administrateur locaux.

L'accès distant à un compte administrateur doit être proscrit.

Les authentifiants d'administration génériques non nominatifs font l'objet d'un séquestre auprès du RSSI. Cette démarche a pour but d'assurer la continuité d'activité, en cas de décès ou d'absence prolongée de la personne les détenant.

Les comptes de services créés pour des besoins applicatifs, sont cartographiés afin de maitriser leur utilisation et font l'objet d'une restriction des droits selon le principe du moindre privilège.

Les comptes de services et d'administration sont désactivés et supprimés dès lors que leur existence n'est plus utile et font l'objet d'une revue annuelle, a minima.

Le cycle de vie des comptes d'administration ne suit pas celui des comptes utilisateurs. En effet, la fermeture d'un compte d'administration est immédiate et intervient le jour même du départ de

l'administrateur. Les mots de passe génériques auxquels il avait accès sont également immédiatement changés.

7.3.3 Cas particulier des domaines Windows

Une politique de gestion des comptes du domaine est documentée et appliquée.

Les groupes « Administrateurs de l'entreprise » et « Administrateurs du domaine » sont restreints au maximum et ne sont accessibles qu'aux seuls personnels administrant le domaine.

7.4 Administration des systèmes

L'accès aux outils et interfaces d'administration doit être strictement limité aux personnes habilitées.

L'habilitation des administrateurs s'effectue selon une procédure définie. A défaut, lorsqu'elle n'existe pas, le responsable hiérarchique de l'agent détermine les habilitations nécessaires à la réalisation des activités qui lui sont confiées.

Les opérations d'administration doivent être tracées et s'appuyer sur des protocoles sécurisés. Celles-ci se feront de façon privilégiée à partir d'un réseau dédié à l'administration et séparé de celui des utilisateurs.

Chaque administrateur est responsable de la sécurité du poste de travail à partir duquel il administre les ressources du SI dont il a la charge. Il évitera toute pratique à risque qui pourrait le compromettre.

Lorsque cela est possible, l'utilisation d'outils centralisés permettant l'automatisation des traitements quotidiens et une vue globale du SI est à privilégier par rapport à l'utilisation d'outils installés directement sur les postes de travail des administrateurs.

La prise en main à distance d'un poste de travail n'est possible que sur autorisation de l'utilisateur et selon les règles définies.

7.5 Envoi en maintenance et mise au rebut

Avant tout envoi en maintenance d'un matériel, les données sensibles non chiffrées doivent être effacées. Il appartient aux propriétaires des données de prévenir en cas de risques sur la sensibilité de celle-ci.

Les supports de données sont effacés avant la mise au rebut de tout matériel.

Les opérations de chiffrement et d'effacement doivent faire appel à des produits qualifiés ou respecter les procédures établies. Dans l'hypothèse de données sensibles, l'effacement consistent en la suppression des données de telle façon qu'elles ne puissent être récupérées par aucun moyen d'aucune sorte.

7.6 Lutte contre les codes malveillants

Un anti-virus doit être déployé sur l'ensemble des serveurs et postes de travail de l'établissement par les équipes techniques de la DSIUN ou des services informatiques en composante.

Les mises à jours des bases antivirales et des moteurs antivirus sont déployées automatiquement.

Les évènements de sécurité de l'antivirus sont envoyés à un serveur central pour analyse statistique et détection des problèmes a posteriori.

Les équipes techniques analysent régulièrement les journaux du serveur central pour détecter au plus tôt un éventuel problème.

7.7 Mise à jour des systèmes et des logiciels

Une procédure de suivi et d'application des correctifs de sécurité pour le périmètre des serveurs, et celui des postes de travail doit être définie et mise en œuvre.

Le processus de gestion des correctifs est adapté suivant les contraintes et le niveau d'exposition du système.

Les systèmes obsolètes doivent être migrés vers une version pour laquelle l'éditeur assure le support et la diffusion des correctifs. A défaut, les systèmes devront être répertoriés par les équipes techniques de la DSIUN ou des services informatiques en composante et isolés du reste du SI.

7.8 Journalisation

Chaque matériel ou application doit permettre la conservation des événements de sécurité.

Les délais de conservation de ces traces sont définis selon la sensibilité des applications et les contraintes légales et réglementaires.

Les équipes techniques de la DSIUN procèdent à la surveillance des comportements anormaux au sein du SI, notamment, par l'analyse des journaux.

Une procédure de gestion et d'analyse des journaux des évènements est définie par le RSSI et validée par le comité de pilotage SSI.

8 Sécurité du poste de travail

8.1 Gestion des postes de travail

8.1.1 Périmètre des postes de travail personnel

Les postes de travail personnel, non achetés sur le budget de l'établissement (ou des co-tutelles ou contrats dans le cas des laboratoires), ne doivent pas être connectés sur le réseau filaire de l'établissement. Le réseau sans fil (WiFi) est le réseau à utiliser pour ces postes de travail. Il est à noter également que la DSIUN n'interviendra pas sur ces postes de travail.

8.1.2 Périmètre des postes de travail des personnels administratifs et techniques

Les postes de travail sont obligatoirement gérés par les équipes techniques de la DSIUN ou des services informatiques en composante, selon les directives de sécurité proposées par la DSIUN et validées par le comité de pilotage SSI restreint.

8.1.3 Périmètre des postes de travail des personnels enseignants / chercheurs

Une offre de service concernant la gestion des postes de travail est proposée par la DSIUN ou les services informatiques en composante, chaque personnel enseignant / chercheur étant libre d'y souscrire ou non.

Dans le cas où un personnel enseignant/chercheur ne souhaiterait pas y souscrire et souhaiterait administrer son poste de travail. Celui-ci devra au préalable en informer le responsable de la structure

propriétaire dudit poste. Qui s'il le souhaite pourra le désigner comme personne administrant techniquement et en toute responsabilité l'équipement.

Dans cette hypothèse, les services informatiques sont déchargés de la responsabilité de la gestion du poste de travail et l'administrateur désigné s'engage à respecter les directives de configuration en termes de sécurité proposées par la DSIUN et validées par le comité de pilotage SSI restreint.

8.1.4 Périmètre des salles pédagogique

Les postes de travail sont gérés par les équipes techniques de la DSIUN ou des services informatiques en composante, selon les directives de sécurité proposées par la DSIUN et validées par le comité de pilotage SSI restreint.

8.2 Identification du poste et inventaire

Un inventaire des postes de travail permettant a minima de connaitre : l'administrateur ou le service informatique en charge de l'équipement, son emplacement, sa destination et une référence de commande doit être maintenu à jour. Pour cela la DSIUN réalisera régulièrement des audits en collaboration avec les directeurs des différentes structures de l'établissement.

8.3 Gestion des privilèges sur les postes de travail

Dans le cas où le poste de travail (portable ou fixe) est géré par les services informatiques, l'utilisateur final ne dispose pas des privilèges d'accès « administrateur ». Dans l'hypothèse où un utilisateur dans le cadre de ses missions aurait besoin d'un accès « administrateur », son responsable hiérarchique devra formuler une demande écrite motivée et justifiée auprès de la DSIUN. Cet utilisateur s'engagera notamment à respecter l'alinéa 3 du chapitre 8.1.3 relatif à l'engagement de l'administrateur délégué. Après analyse de la DSIUN, cette demande devra être validée par le DGS.

Selon le principe du « moindre privilège », une session de travail doit s'effectuer avec un compte sans privilèges. Les privilèges d'accès administrateur ne doivent être utilisés que pour réaliser des tâches d'administration le nécessitant.

Le compte administrateur local est strictement réservé aux services informatiques en charge de la gestion du poste de travail.

8.4 Protection des informations

Les données professionnelles sont obligatoirement stockées sur les espaces centralisés dédiés à cet usage et sauvegardés (NAS monEspace et NAS services) proposés par la DSIUN ou ceux proposés par les services informatiques en composante.

Dans le cas où un utilisateur souhaite pouvoir travailler de façon déconnectée, il est de sa responsabilité de s'assurer de la sécurité et de la sauvegarde des données stockées sur le poste de travail (portable par exemple). Dans le cas de données sensibles il peut se rapprocher de la DSIUN pour étudier leur sécurisation. La sensibilité des données doit être évaluée par l'utilisateur et/ou le directeur de sa structure de travail.

Dans le cas particulier d'un poste de prêt (dont les classes mobiles), les données doivent être supprimées avant sa restitution. Le poste sera réinstallé entre deux prêts.

La réaffectation d'un poste de travail entraine obligatoirement sa réinitialisation.

Toute utilisation d'outils ou services externes tels que Dropbox, Google docs, Google Forms, Google Agenda, Gmail, etc qui conduisent à faire transiter ou à déposer des informations professionnelles et/ou pédagogiques hors des supports et des services offerts par l'université engage la responsabilité de celui qui les utilise. En effet, ces pratiques présentent un risque de vulnérabilité particulier du point de vue, d'une part, de la confidentialité des données, d'autre part de la protection du patrimoine scientifique, technique et littéraire mais également des libertés individuelles.

On apportera une attention toute particulière aux supports amovibles :

Les supports amovible type clé USB ou disques durs externes, représentent un risque non négligeable (code malveillant, vol de données, destruction de matériel, etc.), leur utilisation requiert la plus grande vigilance et nécessite quelques précautions :

- Ne jamais brancher un support amovible non connu sur un poste de travail ;
- Avoir un anti-virus à jour permettant l'analyse des fichiers contenus et/ou exécutés ;
- Dans la mesure du possible dédier un poste de travail pour la récupération des documents sur clés USB (reprographie, bibliothèque, salles pédagogiques, etc.).

8.5 Nomadisme

Le nomadisme s'entend en premier lieu pour les personnes utilisant des périphériques mobiles (ordinateur portable, tablette, téléphone, etc.) en dehors de l'université ou d'un contexte de télétravail, en particulier lors de mission à l'étranger.

La connexion au réseau interne de l'université depuis un réseau extérieur se fait exclusivement au travers de la passerelle d'accès sécurisé (VPN) de l'établissement.

Le personnel en déplacement veillera à consulter et à suivre dans la mesure du possible le passeport voyageur de l'ANSSI.

Et tout particulièrement on citera :

Les périphériques mobiles sont de par nature fortement exposés au vol et à la perte, il convient donc d'être particulièrement vigilant. Il est recommandé de ne pas les laisser sans surveillance lors des déplacements et de limiter le stockage local de données au strict nécessaire et de s'assurer de leur sécurité et sauvegarde.

Si un utilisateur est amené à stocker des données sensibles sur un périphérique mobile, il peut se rapprocher de la DSIUN pour étudier leur sécurisation. La sensibilité des données doit être évaluée par l'utilisateur et/ou le directeur de sa structure de travail.

En cas de perte d'un périphérique mobile, il est impératif de le signaler au RSSI et de procéder au changement de son mot de passe dans les plus brefs délais.

L'utilisation des réseaux sans fil (WiFi) public n'est pas sans risque, il est obligatoire d'avoir un anti-virus à jour, un pare-feu actif, recommandé de désactiver tout partage de fichier et de consulter uniquement des sites sécurisés (https) ou non sensibles. De plus afin de sécuriser les échanges sur ce type de réseau, la passerelle d'accès sécurisé (VPN) de l'établissement sera préférentiellement utilisé.

Les lieux publics mettent à disposition des bornes de rechargement, leur utilisation peut comporter un risque de vol de données, leur usage est à éviter.

9 Sécurité du développement des systèmes

La sécurité doit être prise en compte dès la conception d'un projet de développement logiciel.

Les applications sont sécurisées en cohérence avec la sensibilité des informations traitées et échangées. Les environnements de développement et de pré-production sont distincts de l'environnement de production.

En cas de recours à un prestataire extérieur, on appliquera les consignes du chapitre 4.5 « Gestion des prestataires ».

9.1 Dans le cas de l'acquisition d'un progiciel

Préférer des prestataires respectant les bonnes pratiques de développement logiciel notamment en ce qui concerne la sécurité.

Porter une attention particulière sur son intégration au SI et sur les méthodes d'authentification, de gestion des mots de passe, de gestion des rôles, de sécurisation des accès aux informations, proposées par l'application.

9.2 Dans le cas de développement spécifique

Si le développement est confié à un prestataire, des clauses SSI doivent être intégrées dans le contrat le liant à l'établissement.

Le prestataire s'engage, notamment, à respecter les règles de développement qui s'imposent aux développeurs internes.

Règles de développement préconisées :

- Avoir suivi une formation (au minimum être sensibilisé) au développement sécurisé afin d'éviter les vulnérabilités classiques ;
- S'engager à suivre les règles de bonnes pratiques publiées par l'OWASP et l'ANSSI,
- Utiliser des outils de développement permettant de minimiser les erreurs introduites durant le développement (utilisation de bibliothèques, contrôle des données en entrées, analyse de code, chiffrement des mots de passe stockés) ;
- Rédiger une documentation technique permettant la reprise du développement par un autre développeur ;
- Mettre à disposition de la DSIUN les sources de l'application ;
- Réduire l'adhérence de l'application vis-à-vis de l'environnement sur lequel elle repose, il est nécessaire de pouvoir faire évoluer l'environnement en cas de découverte de vulnérabilités sur celui-ci (version php, version os, version base de données, etc.) ;
- Mettre en œuvre une gestion fine des rôles concernant l'accès aux données à caractère personnel (DCP) ;
- Journaliser les accès et les actions à auditer permettant l'analyse d'une attaque ou d'un dysfonctionnement. Les délais de rétention sont définis selon la sensibilité de l'application et conformément à la législation en vigueur ;

- Se conformer au cadre légal et règlementaire relatif à la protection des données personnelles (RGPD, loi Informatique et Libertés modifiée, etc.)
- S'engager à maintenir, faire évoluer l'application et corriger les vulnérabilités qui seraient découvertes.

9.3 Applications à risques

Les applications à risques si elles ne sont pas à destination d'usagers externes ne sont pas directement accessibles sur internet, mais uniquement via la passerelle d'accès sécurisé (VPN) de l'établissement ou au travers d'un mécanisme de reverse proxy.

10 Traitement des incidents

Un incident SSI peut être défini comme tout événement inhabituel, indésirable ou inattendu, présentant une probabilité forte de compromettre le fonctionnement normal d'un service numérique (interruption ou diminution de la qualité), les activités de l'établissement ou la sécurité de l'information.

Sont notamment considérés comme incidents de sécurité, le vol ou la perte d'un matériel informatique (poste de travail fixe, ordinateur portable, smartphone, …), la divulgation de données, les connexions illicites, la compromission d'un compte numérique, une attaque ciblée de filoutage, la modification frauduleuse de page web, un incident de production dû à un problème logiciel ou matériel, l'infection d'un poste de travail par un code malveillant, les attaques informatiques, etc.

En cas d'alerte de sécurité identifiée au niveau national, le RSSI s'assure de la bonne application des exigences formulées par les instances nationales au niveau de l'établissement dans les meilleurs délais.

10.1 Surveillance du système d'information et détection des incidents

Des mesures organisationnelles et techniques comme des outils de supervision, consoles anti-virus centralisées, analyses des traces, contrôles d'intégrité des systèmes, détections d'intrusion, etc. sont mises en œuvre pour permettre la détection des incidents au plus tôt.

Il appartient aux équipes techniques de la DSIUN de réaliser une surveillance régulière (en période d'ouverture de l'établissement et en heures ouvrées) des systèmes et du réseau dans son périmètre et de revoir périodiquement les différents journaux à la recherche d'anomalies pouvant être révélatrices d'incidents. D'analyser et traiter ces anomalies et d'en faire part dans les meilleurs délais aux DSI et RSSI.

Il appartient aux équipes de la DPST de réaliser une surveillance continue de l'intégrité physique des locaux abritant les biens du SI (température, énergie, détection d'intrusion, vidéo-protection) d'analyser et traiter les anomalies et d'en faire part dans les meilleurs délais aux DSI et RSSI.

10.2 Signalement des incidents de sécurité

Tout usager du système d'information de l'établissement est tenu de signaler le plus rapidement possible tout évènement ou faille de sécurité pouvant impacter la sécurité du SI à son responsable hiérarchique ou au RSSI qui s'assurera de la transmission de l'information le cas échéant aux DSI, président, FSD, DPD, etc.

Le RSSI maintient la liste des incidents survenus et produit un tableau de bord permettant le suivi des incidents de sécurité à destination du comité de pilotage SSI. En cas d'incident de sécurité suffisamment avéré et constitutif d'une violation de donnée à caractère personnel, le RSSI « documente l'incident » : il consigne les faits concernant la violation, ses effets et les mesures prises pour y remédier. Il adresse ensuite cette documentation au DPD afin que celui-ci notifie la violation de données à la CNIL.

La chaîne fonctionnelle SSI est informée de tout incident de sécurité et contribue si nécessaire à son traitement.

Tout incident de sécurité ayant ou pouvant avoir un impact hors établissement, doit être signalé à la chaine SSI ministérielle.

En cas de risque élevé pour les personnes concernées par l'incident, le responsable de traitement doit informer, en des termes clairs et simples, les utilisateurs touchés par l'incident, sauf si le responsable a pris préalablement ou postérieurement à la violation des mesures techniques et organisationnelles appropriées.

10.3 Processus de gestion des incidents

La gestion des incidents suit le processus suivant : détection / signalement, analyse, diagnostic, résolution, rétablissement du service affecté, validation des mesures correctives, bilan et communication.

Selon l'importance de l'incident une fiche de traitement est établie lors de la phase de bilan, afin d'analyser, d'identifier les faiblesses et définir les mesures préventives et correctives permettant d'en limiter la répétition ou les impacts. Les fiches de traitement permettent également d'établir des fiches réflexes mises à disposition des usagers.

Les traces et éléments susceptibles de servir de preuve sont conservés et éventuellement transmis au CERT-RENATER pour analyses complémentaires.

11 Continuité d'activité du système d'information

Un plan de continuité d'activité (PCA) a pour objectif de maintenir les activités essentielles d'un établissement sans interruption de service ou avec une légère dégradation. Par exemple, dans le cadre du système d'information les informations doivent être accessibles en continu.

Un plan de reprise d'activité (PRA) a pour objectif d'assurer la reprise des activités après une défaillance ou un sinistre majeur. Par exemple, dans le cadre du système d'information, cela implique de reconstruire le SI ou basculer sur un système de secours sur une durée déterminée.

Dans la suite de ce chapitre on utilisera le terme PRI pour faire référence au plan de reprise d'activité du système d'information.

11.1 Définition du plan de reprise d'activité du système d'information (PRI)

L'objectif du PRI est de définir et mettre en œuvre, l'organisation permettant de répondre aux incidents majeurs afin de rapidement revenir à un état fonctionnel acceptable. Ceci dans l'optique de palier à tout arrêt prolongé des systèmes et applications critiques, minimisant ainsi l'impact d'un sinistre sur l'activité de l'établissement.

Le PRI est formalisé dans un document décrivant les rôles et responsabilités des intervenants ainsi que les modalités de déclenchement du PRI : basculement en mode dégradé ou sur des solutions de secours en cas de réalisation de l'un des incidents envisagés.

En accord avec la gouvernance, les DSI et RSSI définissent les objectifs du PRI : sinistres à prendre en compte, durée maximale nécessaire à la remise en production (RTO), période acceptable de données non récupérables (RPO), priorité des services à rétablir, etc.

Les équipes techniques définissent l'architecture et les mesures techniques et organisationnelles à mettre en œuvre. Elles rédigent les procédures opérationnelles nécessaires à la mise en œuvre du PRI.

11.2 Mise en œuvre du plan de reprise d'activité du système d'information

Le RSSI assure le suivi de la mise en œuvre du PRI et rend compte au comité de pilotage SSI.

Les équipes techniques mettent en œuvre l'architecture, les mesures techniques et organisationnelles ainsi que les procédures définies dans le PRI. Elles en assurent la supervision et la maintenance au quotidien.

11.3 Maintien en conditions opérationnelles du plan de reprise d'activité du système d'information

La pertinence et l'efficacité du PRI doit être testé et validé au minimum une fois par an dans le cadre d'exercices.

Le RSSI s'assure de la réalisation de ces exercices et de la mise à jour régulière du PRI.

12 Conformité, audit, inspection, contrôle

12.1 Conformité avec les exigences légales et réglementaires

12.1.1 Respect des droits de propriété intellectuelle

Des contrôles sont régulièrement effectués afin de vérifier le respect de la réglementation concernant le téléchargement d'œuvres protégées et l'usage des logiciels. Il est de la responsabilité de l'utilisateur de conserver les preuves d'achat des matériels et logiciels utilisés n'ayant pas été fournis par la DSIUN ou les services informatiques de composante. En cas de manquement caractérisé, des poursuites ou sanctions peuvent être engagées à l'encontre des contrevenants.

12.1.2 Protection des données à caractère personnel

Dans le cadre de la loi, le DPD représente la Commission Nationale Informatique et Libertés (CNIL) dans l'établissement. Toute personne mettant en œuvre un traitement de données au sein de l'établissement doit prendre contact avec celui-ci impérativement dès la phase de conception du projet et avant sa mise en œuvre.

Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise

à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

12.1.3 Protection des enregistrements

Des mesures organisationnelles et techniques sont définies et mises en œuvre afin de protéger les enregistrements (journaux d'événements, activités des dispositifs de contrôles d'accès, archives de vidéosurveillance, etc.) conformément à la réglementation.

12.2 Conformité à la PSSIE et à la PSSI

La conformité à la PSSIE fait l'objet d'un document d'évaluation de l'application des mesures de sécurité transmis au Fonctionnaire de la Sécurité des Systèmes d'Information (FSSI) du ministère. Les indicateurs d'application des mesures et les indicateurs thématiques sont ensuite consolidés au niveau du ministère puis transmis à l'ANSSI.

La conformité à la PSSI de l'établissement est vérifiée par des contrôles réguliers (surveillance dans le cadre de l'exploitation, revue des droits d'accès, analyse des logs système et réseau, analyse des incidents de sécurité, remontées des utilisateurs, …).
Le RSSI s'assure de la mise en œuvre effective des règles de sécurité prévues par la PSSI.
Il établit un bilan annuel de l'état d'avancement de sa mise en œuvre qu'il transmet au comité de pilotage SSI.

12.3 Audits internes et externes

Sous la responsabilité du DSI et du RSSI, des audits de sécurité du système d'information internes et/ou externes sont réalisés régulièrement afin d'identifier les faiblesses et mesurer l'efficacité des mesures mises en œuvre. Ces audits portent sur les aspects techniques (architecture, systèmes, applications, réseaux, sécurité physique, ...) et organisationnels (procédures liées à la sécurité, suivi de la sécurité dans les contrats, …) mis en œuvre.

Les résultats de ces audits font l'objet d'une analyse et de plans d'actions permettant de réviser, améliorer les procédures et mesures de sécurité mises en œuvre, et sont formalisés et soumis au comité de pilotage. Le suivi de la mise en œuvre du plan d'action est de la responsabilité du DSI et/ou RSSI.

A minima tous les trois ans un audit externe doit être réalisé par des experts dûment habilités.

Sous l'autorité du RSSI des tests de vulnérabilités logiques sont effectués fréquemment sur les services (applications/serveurs) accessibles via internet. Les vulnérabilités identifiées font l'objet de corrections immédiates par les équipes en charge de ceux-ci, aidées si besoin, par des experts du domaine. Le retrait d'un service numérique jugé trop vulnérable peut être envisagé selon les risques encourus par l'établissement.

Le RSSI réalise un bilan annuel des tests de vulnérabilités et corrections apportées qu'il transmet au comité de pilotage.

Les outils d'audit (logiciels ou fichiers de données) sont séparés des systèmes en exploitation et ne sont accessibles que par les personnes habilitées. Les outils et résultats des audits sont considérés comme sensibles.

13 Glossaire

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
AQSSI	Autorité Qualifiée pour la SSI (président de l'université)
CERT-RENATER	Centre d'alerte et de réaction aux attaques informatiques des membres du groupement d'intérêt public RENATER
CIL	Correspondant Informatique et Liberté (fonction remplacée par le DPD)
CNIL	Commission nationale de l'informatique et des libertés
CTEP	Comité Technique d'Etablissement Public
DAJI	Direction des Affaires Juridiques et Institutionnelles
DAS	Direction administrative de site
DCP	Données à caractère Personnel
DEVE	Direction des Etudes et de la Vie Etudiante
DGS	Directeur Général des Services
DIREP	Direction de la Recherche et des Projets
DSI	Directeur du Système d'Information
DSIUN	Direction du Système d'Information et des Usages Numériques
DPD	Délégué à la Protection des données (anciennement CIL)
DPST	Direction du Patrimoine et des Services Techniques
DRH	Directeur des Ressources Humaines
DRH	Direction des Ressources Humaines
FSD	Fonctionnaire de Sécurité de Défense
FSSI	Fonctionnaire de la Sécurité des Systèmes d'Information
HFDS	Haut Fonctionnaire de Défense et de Sécurité
OWASP	Open Web Application Security Project
PCA	Plan de Continuité d'Activité
PPST	Protection du Potentiel Scientifique et Technique de la nation
PRA	Plan de Reprise d'Activité
PRI	Plan de Reprise Informatique
PSSIE	Politique de Sécurité des Systèmes d'Information de l'Etat
PSSI	Politique de Sécurité du Système d'Information
RENATER	Réseau National de télécommunications pour la Technologie l'Enseignement et la Recherche
RGPD	Règlement Européen sur la protection des données
RPO	Recovery Point Objective (période acceptable de données non récupérables)
RSSI	Responsable de la Sécurité du Système d'Information
RTO	Recovery Time Objective (durée maximale nécessaire à la remise en production)
SA2I	Service Audiovisuel Informatique de l'IUT
SI	Système d'Information
SSI	Sécurité du Système d'Information
VPN	Virtual Private Network (passerelle d'accès sécurisé)
WIFI	Wireless Fidelity (réseau sans fil)
ZRR	Zone à Régime Restrictif