UNIVERSITÉ DE PAU ET DES PAYS DE L'ADOUR

Politique générale de sécurité de l'information (PGSI)

Approuvée par le Conseil d'administration du 14 mars 2024

Sommaire

1 AVANT-PROPOS

1.1 Évolution du numérique

L'UPPA a développé ses usages du numérique depuis l'ouverture d'Internet en 1995. Le cyberespace et les outils afférents ont ouvert de nouvelles possibilités de communication et de collaboration. Alors que les pratiques numériques se sont mises en place et ont évolué, la quantité d'informations traitées devenait toujours plus importante ainsi que les flux de communication inhérents.

Aujourd'hui l'Information est au centre des activités – on évoque la société de l'information – qui constitue une valeur scientifique et patrimoniale qu'il est important de protéger.

La direction de l'établissement a fait le choix de s'investir dans la protection de ce patrimoine immatériel : l'AQSSI a nommé son Responsable du Management de la Sécurité et l'Information (RMSI) et lui a remis une lettre de mission qui décrit les attendus en matière de protection de l'information.

1.2 La sécurité de l'information (SécInfo) vue par l'UPPA

Tous les métiers qui contribuent aux missions de l'UPPA sont concernés dès lors qu'ils produisent, traitent ou échangent de l'information numériquement. Cette information, qui a un statut d'actif dématérialisé, englobe les données, les outils qui les traitent ainsi que les matériels qui portent ces outils.

La direction de l'établissement a décidé de protéger son patrimoine informationnel face aux risques pouvant impacter ses orientations stratégiques, ou pouvant affecter la réalisation de ses missions.

Pour ce faire, l'établissement s'est fixé l'objectif de mettre en place une politique de management de la sécurité de l'information permettant de :

- respecter les obligations légales, réglementaires et contractuelles ;
- développer la culture de la sécurité de l'information au sein de l'établissement ;
- anticiper et gérer les incidents liés à la sécurité des systèmes d'information, de manière à en atténuer les effets ;
- assurer la protection du potentiel scientifique et technique et le respect des engagements internationaux ;
- protéger les savoir-faire et les données que ce soit de l'enseignement, de la recherche et de sa valorisation ou du pilotage de l'établissement ;
- garantir un statut de partenaire de confiance dans les sphères académique et socio-économique.

La réalisation de ces objectifs passe par la mise en œuvre d'une politique de sécurité de l'information et nécessite l'implication de toutes les parties prenantes telles que les personnels de l'établissement, les personnels vacataires, les étudiants, les prestataires et fournisseurs.

1.3 La PGSI mise en œuvre par l'UPPA

La Politique Générale de Sécurité de l'Information (PGSI) de l'UPPA est produite à partir de la vision stratégique des risques pesants sur l'information dans le cadre des grandes missions de l'établissement :

- la Formation et la Vie Universitaire ;

- la Recherche et l'Innovation ;
- le Pilotage de l'établissement.

Elle constitue le document fondateur du cadre de référence pour l'ensemble des activités et des acteurs de l'UPPA.

2 CHAMP D'APPLICATION

2.1 Contexte légal et réglementaire

L'établissement est responsable de ses informations et doit appliquer les lois et règlements en vigueur sur les différents niveaux d'information, notamment dans le cadre de projets réalisés pour certains Opérateurs d'Importance Vitale (OIV) (Annexe 2 : réglementation relative au niveau d'information).

Ces différentes catégories de réglementations qui régissent la sécurité de l'information, réunissent plus largement les thèmes relatifs à la protection des systèmes d'information, de l'administration électronique ainsi que plus spécifiquement, la cryptographie ou d'autres réglementations techniques (https://www.ssi.gouv.fr : Réglementation/).

2.2 Missions réglementaires

L'université de Pau et des pays de l'Adour est un établissement public à caractère Scientifique, Culturel et Professionnel (EPSCP). À ce titre, ses missions sont définies dans le cadre réglementaire national (Annexe 3 : Extrait du Code de l'éducation.).

Ces missions s'appuient sur des processus de création de nouvelles connaissances dans différents domaines et produisent des informations originales. Il convient de protéger ces connaissances, en fonction de leur niveau de sensibilité.

2.3 Spécificités de l'établissement

L'Université de Pau et des pays de l'Adour organisée en collèges (Annexe 4 : Liste des collèges UPPA) répartis sur les différents campus, est un établissement pluridisciplinaire qui intervient dans trois grands champs disciplinaires :

- Droit, Économie, Gestion, Management,
- Sciences et Technologies,
- Lettres, Langues, Arts, Sciences Humaines et Sport.

L'UPPA est propriétaire du domaine Internet univ-pau.fr qui définit le périmètre d'accès à ses ressources numériques : elle en assure la sécurité afin de préserver ses activités, sa souveraineté et son image de marque.

2.4 Champ d'application et limites

La PGSI de l'UPPA est applicable à la totalité de l'établissement pour :

- l'ensemble de ses informations ;
- l'ensemble de ses activités et processus ;
- l'ensemble de ses systèmes d'information, hébergés en interne ou délégués par contrat ;

- l'ensemble des personnes physiques et morales constituées par :
  - les collaborateurs internes, chercheurs et étudiants ;
  - les partenaires externes (sous-traitants, co-traitants, infogérants, auditeurs, etc.).

La PGSI promeut ainsi la prise en compte de la sécurité de l'information dans l'organisation même de l'établissement et ses interactions avec l'extérieur. Elle s'applique, quel que soit le moyen technique utilisé pour traiter ou stocker cette information.

2.5 Exclusions

Sont exclues les informations classifiées de défense, et pour lesquelles une réglementation spécifique est applicable, et qui est citée en annexe de la présente PGSI.

2.6 Revue de la PGSI

La PGSI de l'UPPA doit être mise à jour a minima annuellement pour tenir compte des évolutions affectant la sécurité de l'information de l'UPPA telles que :

- les évolutions des enjeux et des menaces ;
- les évolutions internes stratégiques, organisationnelles, structurelles ;
- les évolutions réglementaires, juridiques et contractuelles ;
- les évolutions technologiques, des moyens de communication ou de partage d'information.

3 PRINCIPES DE GOUVERNANCE DE LA SÉCURITÉ DE L'INFORMATION

3.1 Principe directeur de la sécurité de l'information

Objectif :
Donner à la sécurité de l'information une orientation stratégique alignée avec les risques métiers

Les missions de l'UPPA l'amènent à construire et délivrer des informations, notamment à potentiel scientifique et technique, et opérer des services pour des étudiants, des entreprises ou des collectivités.

Une compromission de ces informations impacterait la capacité à mener ses missions et pourrait avoir des conséquences humaines, scientifiques ou encore sur les services délivrés.

La sécurité de l'information contribue à préserver la valeur des actifs immatériels de l'UPPA, en ce sens, elle se doit d'assurer :

- la protection des processus et informations dématérialisées de l'établissement ;
- la continuité des activités de l'établissement s'appuyant sur le numérique ;

Ces enjeux reposent sur les principes directeurs suivants :

- les orientations stratégiques de la sécurité de l'information sont alignées avec les grandes missions de l'établissement ;
- la sécurité de l'information est pilotée par les risques ;
- la sécurité de l'information produit des mesures et en contrôle l'efficacité.

3.2 Principe d'organisation pour la sécurité de l'information

Objectif :
Déterminer les rôles et responsabilités pour assurer la maîtrise des risques

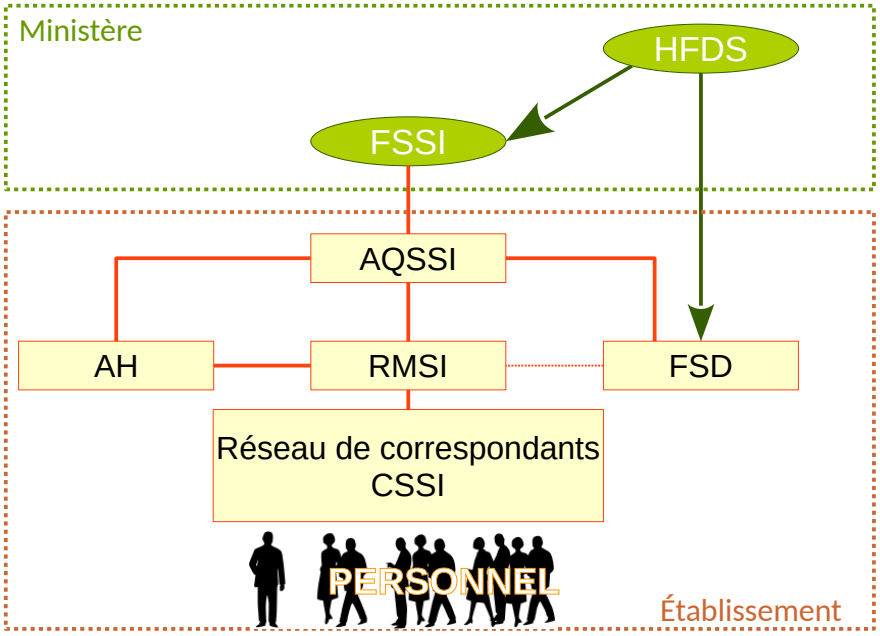
Les **rôles et responsabilités** ci-après détaillent l'ensemble des acteurs de la sécurité de l'information spécifiés au sein de l'UPPA.

3.2.1 Acteurs de la sécurité de l'information

Instances de gouvernance de la sécurité de l'information au niveau de l'État et au sein de l'UPPA

HFDS Haut Fonctionnaire de Défense et de Sécurité
FSSI Fonctionnaire de Sécurité des Systèmes d'Information (un par ministère)
AQSSI Autorité Qualifiée pour la Sécurité des Systèmes d'Information (Président)
AH Autorité d'Homologation
FSD Fonctionnaire Sécurité Défense
RMSI Responsable du Management de la Sécurité de l'Information
CSSI Correspondants de la Sécurité des Systèmes d'Information

Schéma de l'organisation :



3.2.1.1 RMSI (Responsable du Management de la Sécurité de l'Information)

Le RMSI conseille le président et le DGS dans le pilotage de l'établissement sur le volet sécurité de l'information. Il a un rôle d'accompagnement à la maîtrise d'ouvrage (AMOA). Il s'appuie sur les principales maîtrises d'œuvre de la sécurité de l'information représentées par :

- la Direction du Numérique,
- la Direction des Ressources Humaines,
- la Direction du Patrimoine,
- la Direction des Affaires Juridiques.

L'ensemble de ses missions est détaillé dans la lettre de mission que le Président lui a assigné.

3.2.1.2 Réseau des CSSI (Correspondants de la Sécurité des Systèmes d'Information)

Le correspondant SécNum (CSSI) contribue aux tâches de gestion de la SécNum et joue un rôle essentiel d'intégration de la SécNum dans ses activités. Il est le maillon final de la chaîne d'alerte SécNum. À ce titre, il intervient sur le terrain notamment pour la prise en charge et le suivi des incidents.

Il connaît les politiques de SécNum de l'établissement et en assure la prise en compte dans son périmètre géographique et fonctionnel. Il est force de proposition pour les choix technologiques qui vont réaliser les mesures de sécurité. Il évalue les moyens nécessaires à la réalisation de ces mesures.

Le CSSI informaticien est en mesure d'appliquer les recommandations de sécurité émises par le CERT[1]. Dans ce cadre, il est capable de concevoir une solution ou un contournement dans son domaine technique et d'en faire la proposition au RMSI pour validation.

Ses compétences techniques étant reconnues, il peut être sollicité par le RMSI pour participer, s'il le souhaite, à la réflexion sur l'organisation de la SécNum de l'établissement.

Il établit un dialogue avec les collègues auprès desquels il intervient.

3.2.2 Détail des Instances de gouvernance de la sécurité de l'information

Les instances spécifiées ci-après sont des instances de conseil sur leur périmètre d'action. Elles sont permanentes et contribuent au dispositif relatif à la sécurité de l'information.

<table>
<tr><td colspan="4">COMITÉ DE PILOTAGE STRATÉGIQUE SÉCNUM</td></tr>
<tr><td>Objectif</td><td colspan="3">Accompagner l'AQSSI dans le pilotage de la sécurité de l'information</td></tr>
<tr><td>Participants</td><td>• Sous la responsabilité de l'AQSSI
• Animé par le RMSI
• Composé de membres permanents :
○ Président
○ DGS
○ VP du conseil d'administration
○ VP Numérique
○ Directeur du Numérique
○ DPO
○ FSD
• Participation de membres consultatifs sur invitation</td><td>Périodicité</td><td>1 à 3 par an</td></tr>
</table>

COMITÉ DE PILOTAGE OPÉRATIONNEL SÉCNUM	
Objectif	• Évolution de la PSSI, analyse et traitement des risques, processus de suivi • Animation/participation aux groupes de travail Sécurité du Numérique

1 Computer emergency response team : centre d'alerte et de réaction aux attaques informatiques, destiné aux entreprises ou aux administrations, mais dont les informations sont généralement accessibles à tous.

	• Relais des décisions de Sécurité du Numérique vers les composantes • Gestion des incidents		
Participants	• Sous la responsabilité du RMSI • Animé par le RMSI • Composé des CSSI	Périodicité	2 à 4 par an

CELLULE PROTECTION SÉCURITÉ			
Objectif	• Hébergement des fonctions DPO, FSD et RMSI • Conseil auprès du président pour les questions relevant de la sécurité de défense, de la sécurité du numérique et de la protection des données à caractère personnel.		

Participants	• Sous la responsabilité du DGS
	• Animé par le DGS
	• Composés de membres permanents
	  ○ DGS / DGS-A
	  ○ DPO
	  ○ FSD
	  ○ RMSI
	  ○ VP CA
		Périodicité	1 par mois

3.3 Principe de pilotage par les objectifs de sécurité

Objectif :
Assurer l'amélioration continue du dispositif relatif à la sécurité de l'information dans le cadre d'un SMSI

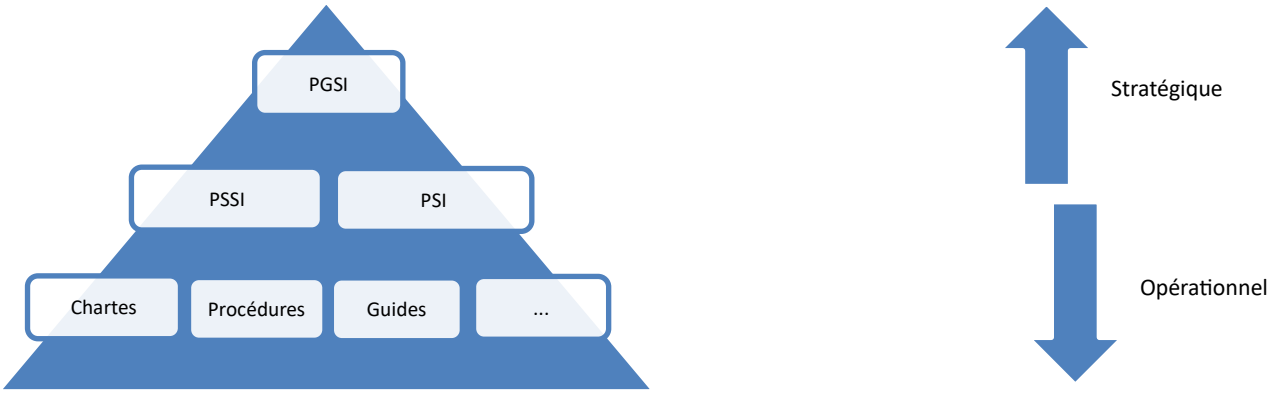
3.3.1 Cadre de référence de la sécurité de l'information

Ce cadre est élaboré et maintenu à jour, pour offrir à l'ensemble des parties prenantes, des repères explicites pour la prise en compte de la sécurité de l'information dans leurs activités. Il constitue un socle homogène et maîtrisé pour assurer un niveau de sécurité de l'information adapté à toutes les entités de l'établissement.

La PGSI (politique générale de sécurité de l'information) de l'UPPA constitue ainsi le document fondateur de ce cadre de référence, et doit être déclinée en :

- une PSSI UPPA incluant un volet ZRR (zone à régime restrictif) ;
- une PSI de façon à intégrer les périmètres PPST et protection des données à caractère personnel ;
- les chartes des utilisateurs et des administrateurs du numérique.

L'établissement s'appuie sur la PGSI afin de mener et de compléter sa démarche sécurité de l'information par la construction des éléments suivants :



3.3.2 Pilotage par les risques de la sécurité de l'information

La sécurité de l'information est pilotée par les risques au niveau de chaque mission de l'UPPA. En ce sens, à chacun des niveaux concernés, les risques sécurité de l'information sont identifiés et des plans d'actions sont élaborés en réponse à ces risques.

Pour mener à bien la gestion des risques, la démarche conseillée par l'ANSSI (agence nationale de la sécurité des systèmes d'information) et mise en œuvre par l'UPPA est la méthode d'analyse de risque EBIOS RM (Expression des Besoins et Identification des Objectifs de Sécurité risk manager).

Pour l'établissement, les risques d'une atteinte à la disponibilité, l'intégrité ou la confidentialité des informations se traduisent par des impacts potentiels majeurs, contre lesquels il convient de se prémunir.

Face à des risques, il convient d'identifier les actifs et processus qui doivent être protégés, de quantifier l'enjeu correspondant, de formuler des objectifs de sécurité et d'identifier, arbitrer et mettre en œuvre les actions adaptées au juste niveau de risque acceptable.

Ces éléments seront analysés et formulés sous forme de règles dans la politique de sécurité des systèmes d'information (PSSI-UPPA).

3.3.3 Audit et contrôle de la sécurité de l'information

La sécurité de l'information est évaluée de manière continue et contrôlée annuellement au niveau de l'UPPA, et de chaque mission.

La cible de sécurité est élaborée chaque année par le RMSI afin de favoriser l'amélioration continue de la sécurité de l'information tout en assurant une approche proportionnée à la maturité des entités face à chacune des missions.

La démarche de contrôle peut être soutenue par des audits réguliers (par exemple, recherche systématique de vulnérabilités exposées sur Internet) ou ponctuels (cas de l'homologation) de sécurité de l'information, internes ou externes. Le référentiel d'exigences relatif aux prestataires d'audit de la sécurité des systèmes d'information (annexe C du RGS) fixe les règles que doivent respecter les prestataires tiers qui réalisent des audits de la sécurité des systèmes d'information des autorités administratives.

3.3.4 Tableaux de bord relatifs à la sécurité de l'information

Des tableaux de bords relatifs à la sécurité de l'information doivent être consolidés au niveau de l'UPPA, de chaque entité et de chaque mission. Au niveau stratégique, le tableau de bord de la sécurité de l'information permet de suivre l'application de la politique de sécurité et de disposer d'éléments propres à qualifier les ressources devant être allouées à la sécurité de l'information.

Les tableaux de bord relatifs à la sécurité de l'information doivent être revus lors des comités sécurité définis au niveau concerné et permettre d'identifier des actions préventives et correctives, le cas échéant.

4 PRINCIPES DE SÉCURITÉ DE L'INFORMATION

Les principes de sécurité spécifiés dans les sections suivantes visent à contribuer à la réalisation des objectifs inhérents en réponse aux risques correspondants identifiés à l'UPPA. Ces principes de sécurité seront par la suite déclinés en règles de sécurité à vocation opérationnelle dans les PSSI.

4.1 Principe de protection de l'information

Objectif :
Maîtriser les informations selon leur niveau de sensibilité tout au long de leur cycle de vie

4.1.1 Classification de l'information

Toute information doit :

- être associée à un propriétaire, responsable de sa classification et des moyens de protection mis en œuvre sur cette information tout au long de son cycle de vie ;
- faire l'objet d'une classification par son propriétaire en accord avec son niveau de sensibilité et doit être marquée en conséquence.

Qu'il s'agisse ou non de données sensibles au sens de la réglementation en vigueur, celles-ci sont évaluées en liaison avec la Déléguée à la Protection des Données Personnelles (DPD) de l'établissement. Cette analyse est conduite selon la méthode définie conjointement par le RMSI et le DPD de l'établissement,

conformément aux dispositions en vigueur et aux instructions de l'autorité de contrôle (CNIL).

Une information peut avoir différents niveaux de classification au cours de son cycle de vie.

La classification de l'information figure en annexe de la PSI (politique de sécurité de l'information).

4.1.2 Protection de l'information tout au long de son cycle de vie

Les moyens de protection de l'information doivent être proportionnés au niveau de classification et adaptés aux conditions spécifiques de travail (mesures de protection physique, pratiques pour la diffusion, etc).

Une attention particulière doit être portée aux informations archivées qui doivent bénéficier d'un niveau de protection suffisant au regard de leur valeur juridique, par exemple pour la signature électronique, de leur valeur scientifique ou d'un intérêt pour le pilotage de l'établissement, par exemple à des fins statistiques.

4.1.3 Protection des informations appartenant à des tiers

Les informations confiées par des tiers à l'UPPA doivent être protégées conformément à leur classification d'origine éventuellement exprimée par leur dépositaire et à toute mention de protection particulière exprimée par celui-ci, notamment contractuelle.

4.1.4 Intégration de la sécurité de l'information dans tous les projets

La sécurité de l'information doit être prise en compte dans les processus projet, si possible, dès la phase d'opportunité ou, obligatoirement, dès la phase de faisabilité de manière proportionnée aux risques de sécurité de l'information. Cette prise en compte est réalisée au travers de l'analyse de risque.

4.1.5 Veille sur les menaces de sécurité et les vulnérabilités

Un dispositif de veille sur les menaces de sécurité de l'information et les vulnérabilités doit être mis en œuvre. Il doit permettre d'identifier les méthodes d'attaque et les failles, pour anticiper les situations de risque auxquelles pourra être confronté UPPA. Il pourra s'appuyer le cas échéant sur un service externe offrant toutes les conditions de sécurité liée à l'infogérance[2].

2 https://www.ssi.gouv.fr/guide/externalisation-et-securite-des-systemes-dinformation-un-guide-pour-maitriser-les-risques/

4.2 Principe de maîtrise des habilitations et du contrôle des accès

Objectif :
Maîtriser l'accès à l'information et à ses moyens de traitement dans tous les processus métiers.

4.2.1 Gestion des habilitations

Tout utilisateur, qu'il soit personnel UPPA, usager ou intervenant extérieur, doit disposer d'une identité numérique unique dès lors qu'il accède au système d'information de l'UPPA.

Les droits associés à son identité numérique doivent être en relation avec ses besoins métiers et selon les principes du moindre privilège.

Les droits de chaque utilisateur et administrateur doivent être modifiés, dès lors que ses attributions évoluent, ou retirés, dès que la relation qui le lie avec l'UPPA se termine.

Les modalités et les processus d'attribution, de modification et de retrait des droits associés aux identités numériques doivent inclure à minima la validation par une autorité compétente d'une demande de droit (autorité d'enregistrement).

Les comptes génériques ou dits « de service » (identité numérique associée à plusieurs utilisateurs) sont interdits par défaut et doivent faire l'objet d'une demande de dérogation explicite et justifiée adressée au Président.

4.2.2 Revue des habilitations

Une revue annuelle des comptes et droits d'accès logiques et physiques doit être effectuée afin de s'assurer que seuls les comptes présents et les droits qui leur sont associés sont légitimes.

4.2.3 Gestion des accès logiques et physiques

Toute personne ou tout utilisateur doit être authentifié dès lors qu'il accède à des locaux de l'UPPA (accès physique) ou au système d'information de l'UPPA (accès logique), en conformité avec les habilitations dont il dispose.

Pour les locaux, un zonage est défini au sein des différents bâtiments en relation avec la Direction du Patrimoine et le responsable du bâtiment. Les niveaux de sécurité applicables aux zones sont décrits dans la PSSI de l'UPPA qui renverra aux chartes, procédures et guides associés.

4.2.4 Traçabilité des habilitations et des accès logiques et physiques

Toutes les modifications apportées aux comptes et aux droits (création / suppression de compte et attribution / modification / retrait de droits) doivent être journalisées.

Toutes les tentatives d'accès logiques ou physiques (réussies ou en échec) doivent être journalisées.

4.3 Principe de sensibilisation et formation des utilisateurs

Objectif :
Développer une culture de la sécurité de l'information au sein de l'UPPA.

4.3.1 Sensibilisation au bon usage du système d'information

Le facteur humain est central dans le processus de sécurité de l'information.

Sont considérés comme « Utilisateur du Numérique », l'ensemble des personnes autorisées en raison de leur statut à accéder et utiliser les moyens numériques de l'établissement accessibles sur le domaine Internet univ-pau.fr :

- Le personnel de l'université, qui comprend toute personne rémunérée par l'UPPA, enseignant, chercheur, enseignant chercheur, BIATSS… devant accéder au système d'information de l'UPPA pour l'exercice de sa mission ;
- Les intervenants extérieurs à l'établissement, vacataires et invités qui disposent d'un compte informatique ;
- Les étudiants qui représentent les usagers de l'établissement.

Les utilisateurs doivent prendre connaissance de la charte des utilisateurs du numérique et la signer. Cette charte et son volet « Sécurité de l'information » doivent être diffusés et accessibles à tous les utilisateurs dès leur intégration.

L'utilisateur est responsable civilement et pénalement du respect des lois et règlements en vigueur. Il doit respecter les règles édictées par l'établissement et signaler tout incident de sécurité numérique qu'il aurait pu constater. Le vice-président du conseil d'administration intervient dans le pilotage stratégique de la sécurité de l'information. Le directeur des ressources humaines intervient dans le pilotage opérationnel de la sécurité de l'information.

4.3.2 Sensibilisation à la sécurité de l'information

Tous les utilisateurs du numérique de l'UPPA doivent être sensibilisés à la sécurité de l'information, pour adopter les bonnes pratiques au quotidien et savoir réagir face à un incident de sécurité de l'information ; par exemple dans le cadre de l'expérimentation numérique (volet recherche).

En particulier, les utilisateurs doivent être informés de la sensibilité des informations de leur activité. Une attention particulière doit être portée aux cas de partage, ainsi qu'aux modes de partage de l'information dans le cadre de recherche ou autres contextes sensibles.

À cet effet, l'UPPA met à disposition des personnels UPPA, usager ou intervenant extérieur et de leurs entités d'appartenance :

- un parcours d'intégration incluant une sensibilisation aux enjeux de la sécurité de l'information au sein de l'UPPA ;
- un programme de communication et de sensibilisation à la sécurité de l'information, défini par la fonction RMSI sur une base pluriannuelle.

4.3.3 Sensibilisation en fin de contrat

Une sensibilisation est mise en œuvre pour les utilisateurs ayant eu accès à des informations sensibles ou de recherche pour le compte de l'UPPA.

Tous les utilisateurs de l'UPPA en fin de contrat ou de cursus doivent faire l'objet d'un rappel de leur devoir de réserve et du contenu de la charte des utilisateurs du numérique qu'ils ont signée à leur arrivée.

4.3.4 Sensibilisation des administrateurs du numérique

Les administrateurs constituent le premier niveau de protection de l'information de l'UPPA. Il est donc nécessaire que ces derniers s'engagent avec l'UPPA dans :

- Le respect de la législation ;
- La préservation de l'intégrité de l'information ;
- L'utilisation rationnelle et loyale des services.

À ce titre, une charte spéciale à l'attention des administrateurs (administrateurs système et administrateurs de leur poste de travail) doit être signée pour engager la responsabilité de ces derniers.

4.4 Principe de protection du Système d'Information

Objectif :
Maîtriser la sécurité du système d'information de l'UPPA sur l'ensemble de son cycle de vie.

4.4.1 Intégration de la sécurité dans l'architecture du système d'information

Dans tout projet de réalisation ou de modification d'un système d'information, le besoin de sécurité doit être pris en compte au même titre que les besoins fonctionnels que vise à satisfaire le système ou l'application.

La sécurité de l'information est à considérer très en amont du projet, dès la phase d'étude de faisabilité, afin d'en augmenter l'efficacité et de diminuer son coût. Ainsi, chaque projet informatique doit réaliser une évaluation préalable des besoins de sécurité associés au cadre réglementaire, à l'hébergement, au stockage et la sauvegarde ou encore aux passerelles Internet.

L'architecture du système d'information doit intégrer la sécurité par conception dans les services qu'elle fournit du début à la fin d'un projet, en tant que support des missions de l'UPPA.

4.4.2 Maîtrise des terminaux ayant accès au système d'information

Les composants du système d'information doivent être maîtrisés par l'UPPA et disposer de fonctions de sécurité pour les protéger, entre autres, contre les codes malveillants, les tentatives d'intrusion, les vols d'informations ou l'exploitation de vulnérabilités.

Les composants mobiles doivent disposer des mêmes fonctions de sécurité, actives en tout lieu, et qu'ils soient connectés ou déconnectés du système d'information (ex : dans le cadre d'affectation de matériel mobile pour les chercheurs). Le cas particulier du matériel non professionnel, par exemple le BYOD[3], doit faire l'objet de mesures spécifiques à étudier selon les situations, étant entendu que les équipes numériques de l'établissement n'interviennent pas sur le BYOD.

Les composants tels que les objets connectés ou la gestion technique des bâtiments doivent disposer de fonctions de sécurité pour les protéger, entre autres, contre le vol des données qu'ils traitent et les modifications inappropriées de leurs systèmes provoquant l'altération ou l'indisponibilité du service qu'ils délivrent.

4.4.3 Maintien en conditions de sécurité du système d'information

Le maintien en conditions de sécurité du système d'Information et de ses composants doit être assuré en toutes circonstances et tout au long de leurs cycles de vie.

À cet effet, les modalités et les processus de maintien en conditions de sécurité doivent être intégrés dans les processus opérationnels du système d'information.

Avant sa mise en service opérationnelle, tout système d'information doit faire l'objet d'une homologation de sécurité par une autorité d'homologation désignée par l'AQSSI.

Par ailleurs, pour renforcer la sécurité de son système d'information, l'établissement doit considérer d'utiliser, lorsque cela est possible, des produits et des offres de services de prestataires certifiés ou

3 BYOD Bring Your Own Device : « apporte ton propre matériel »

qualifiés par l’ANSSI.

4.4.4 Surveillance de la sécurité du système d’information

Les systèmes d’information supportant des activités et des processus critiques de l’UPPA doivent faire l’objet d’une cybersurveillance adaptée visant à remonter les événements de sécurité au sein des systèmes d’information. Cette surveillance doit être interfacée avec le processus de gestion des incidents de sécurité de l’information. Elle s’appuie sur la cartographie du SI de l’établissement.

4.5 Principe de sécurité de l'information dans les relations avec les tiers

Objectif :
Assurer la sécurité de l'information lorsque les activités sont partagées avec un tiers.

4.5.1 Intégration de la sécurité de l'information dans les contrats avec les tiers

Les accords conclus avec des tiers doivent intégrer les principes et les règles applicables (en fonction de la nature du contrat) de la PGSI de l'UPPA, afin d'assurer que les services portés par ce contrat ne dégraderont pas la maîtrise des risques qui pèsent sur l'UPPA.

En particulier, les exigences réglementaires relatives au traitement des données confidentielles ou personnelles doivent faire l'objet de clauses adaptées et proportionnées aux activités sous-traitées dans lesdits accords.

4.5.2 Plan d'Assurance Sécurité des fournisseurs

Dans les cas où l'UPPA fait appel au service d'un tiers, les modalités de mise en pratique des principes et des règles de sécurité par les fournisseurs de l'UPPA doivent faire l'objet d'un document spécifique nommé Plan d'Assurance Sécurité (PAS) annexé au contrat.

4.5.3 Plan d'Assurance Sécurité de l'UPPA

Dans les cas où un tiers fait appel aux services de l'UPPA, par exemple lors d'un projet de recherche en partenariat, les modalités de mise en pratique de ses propres principes et règles de sécurité issues de la PGSI de l'UPPA, mais aussi des exigences du contrat doivent faire l'objet d'un document spécifique (Plan d'Assurance Sécurité ou équivalent) annexé au contrat.

4.6 Principe de continuité d’activité

Objectif :
Assurer la disponibilité d’une information dès lors qu’elle est nécessaire dans un processus métier et les activités associées.

4.6.1 Expression des besoins de continuité d’activité

Toutes les activités portant les missions de l’UPPA doivent être associées à un propriétaire identifié comme référent métier. Le référent métier est responsable de l’expression des besoins de continuité des processus et activités.

4.6.2 Plan de continuité d’activité

Un plan de continuité d’activité doit être défini, mis en œuvre et maintenu, sur les processus et les activités de l’UPPA.

Ce plan de continuité d’activité doit être diffusé aux différentes parties prenantes, et faire l’objet d’exercices de test et de révision réguliers (a minima annuels), avec la participation des parties prenantes désignées.

Les résultats de ces tests doivent être consignés et archivés, et faire l’objet de plan d’action adaptés en fonction des résultats obtenus.

4.7 Principe de gestion des incidents de sécurité de l'information

Objectif :
Assurer une réaction rapide, adaptée et proportionnée à un incident de sécurité de l'information

4.7.1 Gestion des incidents de sécurité de l'information

Les incidents de sécurité de l'information doivent faire l'objet d'un traitement systématique adapté à leur nature et à leur criticité.

La remontée des incidents de sécurité majeurs doit faire l'objet d'une action particulière destinée à informer sans délai la chaîne fonctionnelle sécurité de l'information.

Les incidents de sécurité de l'information sont répertoriés dans le registre des incidents opéré par le réseau de CSSI sous la vigilance du RMSI.

4.7.2 Gestion de crise sécurité de l'information

Un incident de sécurité de l'information présentant des caractéristiques particulières, notamment d'impact ou d'absence de maîtrise, doit pouvoir déclencher un processus de crise.

5 ANNEXES

5.1 Annexe 1 : glossaire

AH :	Autorité d'Homologation
AQSSI :	Autorité Qualifiée pour la Sécurité des Systèmes d'Information (Président)
Besoins de continuité :	Exprimés au travers de : • la durée maximale d'Interruption admissible (DDA). Exprimée en unité de temps, elle correspond à la durée attendue séparant un sinistre de la reprise du service ; • la perte de donnée maximale admissible (PDMA). Exprimé en unité de temps, elle correspond au délai séparant l'âge des données les plus récentes disponibles de la date de survenance du sinistre
CSSI :	Correspondants de la Sécurité des Systèmes d'Information
DPD/DPO :	Déléguée à la Protection des Données Personnelles
FSD :	Fonctionnaire de Sécurité de Défense
FSSI :	Fonctionnaire de Sécurité des Systèmes d'Information (un par ministère)
HFDS :	Haut Fonctionnaire de Défense et de Sécurité
OIV :	Opérateur d'Importance Vitale
Parties prenantes :	Dans le présent document, le terme « parties prenantes » désigne les personnels de l'établissement, les personnels vacataires, les étudiants, les prestataires et fournisseurs
PGSI :	Politique générale de sécurité de l'information
PPST :	Dispositif de Protection du Potentiel Scientifique et Technique
PSI :	Politique de Sensibilité de l'Information
RGPD :	Règlement Général sur la Protection des Données. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).
RGS :	Référentiel Général de Sécurité
RMSI :	Responsable du Management de la Sécurité et l'Information
RSSI :	Responsable de la Sécurité des Systèmes d'Information
Système d'Information :	Ensemble des moyens mis en œuvre par l'établissement pour opérer les services nécessaires à ses missions et qui traitent les informations de gestion, d'enseignement et de recherche.

5.2 Annexe 2 : réglementation relative au niveau d'information

Plus les informations sont sensibles et plus les règles de protection des systèmes d'information sont contraignantes. Voici un système de représentation par niveau de sensibilité, texte et entité concernée. (Source : ANSSI)

Sensibilité	Textes	Entités concernées
Informations, secret de la défense nationale	IGI 1300 IGI 2100 / 2102 II 920 II 300	Entités privées ou publiques concernées par la gestion d'information liée au secret de la défense nationale
Informations Diffusion restreinte	Instruction n°901 sur la protection des SI sensibles (partie 1 + partie 2)	Entités publiques ou privées qui traitent des informations de mention « Diffusion Restreinte » Entités mettant en œuvre des zones à régime restrictif (ZRR) et concernées par les spécialités les plus sensibles dans le cadre du dispositif relatif à la protection du potentiel scientifique et technique de la Nation
	RGS	Autorités administratives échangeant des informations avec les usagers et entre autorités administratives
	II 300 – Annexe 2	Entités publiques ou privées qui traitent des informations de mention
Informations sensibles	Instruction n°901 sur la protection des SI sensibles (partie 1)	Entités publiques ou privées soumises à la réglementation relative à la PPST (Protection du potentiel scientifique et technique) pour leurs SI liés à une ZRR.
	PSSIE	Administrations de l'État
	RGS	Autorités administratives échangeant des informations avec les usagers et entre autorités administratives
	II 300 – Annexe 2	Administrations de l'État
Informations peu sensibles	PSSIE	Administrations de l'État
	RGS	Autorités administratives échangeant des informations avec les usagers et entre autorités administratives
Informations liées à une réglementation spécifique	Exemples : Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés Arrêté du 3 juillet 2012 relatif à la protection du potentiel scientifique et technique de la nation	En fonction du texte

5.3 Annexe 3 : Extrait du Code de l'éducation.

L'Article L123-3 (modifié par la LOI n°2013-660 du 22 juillet 2013 – art. 7) reprend les missions de l'université :

1. La formation initiale et continue tout au long de la vie ;
2. La recherche scientifique et technologique, la diffusion et la valorisation de ses résultats au service de la société. Cette dernière repose sur le développement de l'innovation, du transfert de technologie lorsque celui-ci est possible, de la capacité d'expertise et d'appui aux associations et fondations, reconnues d'utilité publique, et aux politiques publiques menées pour répondre aux défis sociétaux, aux besoins sociaux, économiques et de développement durable ;
3. L'orientation, la promotion sociale et l'insertion professionnelle ;
4. La diffusion de la culture humaniste, en particulier à travers le développement des sciences humaines et sociales, et de la culture scientifique, technique et industrielle ;
5. La participation à la construction de l'Espace européen de l'enseignement supérieur et de la recherche ;
6. La coopération internationale.

5.4 Annexe 4 : Liste des collèges UPPA

Collège EEI : Études Européennes et Internationales

Implanté sur le campus de Bayonne et de Pau, ce collège héberge des composantes internes de formation et de recherche, une école doctorale et des services administratifs.

Collège SSH : Sciences Sociales et Humanités

Implanté sur les campus d'Anglet, de Pau et de Tarbes, ce collège héberge des composantes internes de formation et de recherche, une école doctorale et des services administratifs.

Collège STEE : Sciences et Technologies pour l'Énergie et l'Environnement

Implanté sur les campus d'Anglet, Bayonne, Mont-de-Marsan, Pau,et Tarbes, ce collège héberge la totalité des composantes internes de formation (dont deux IUT et des écoles d'ingénieurs) et de recherche, une école doctorale, un centre de service instrumental et des services administratifs.