

Politique de Sécurité des Systèmes d'Information (PSSI)

Approuvée par le Conseil d'administration du 14 mars 2024

Sommaire

1. Domaine d'application.....	3
1.1. Contexte.....	3
1.2. Périmètre.....	3
1.3. Les besoins en sécurité de l'UPPA.....	4
2. Mise en application de la sécurité des systèmes d'information.....	4
2.1. Pilotage par les objectifs de sécurité des systèmes d'information.....	4
2.2. Le cadre de référence de la sécurité l'information pour l'UPPA.....	4
2.2.1. Guide d'hygiène informatique de l'ANSSI.....	4
2.2.2. La Politique de Sécurité des Systèmes d'Information de l'État.....	4
2.2.3. Politique Générale de Sécurité de l'Information.....	5
2.2.4. La Politique de Sécurité de l'Information.....	5
2.2.5. Le règlement intérieur et les chartes.....	5
2.3. Accès aux mesures de sécurité.....	5

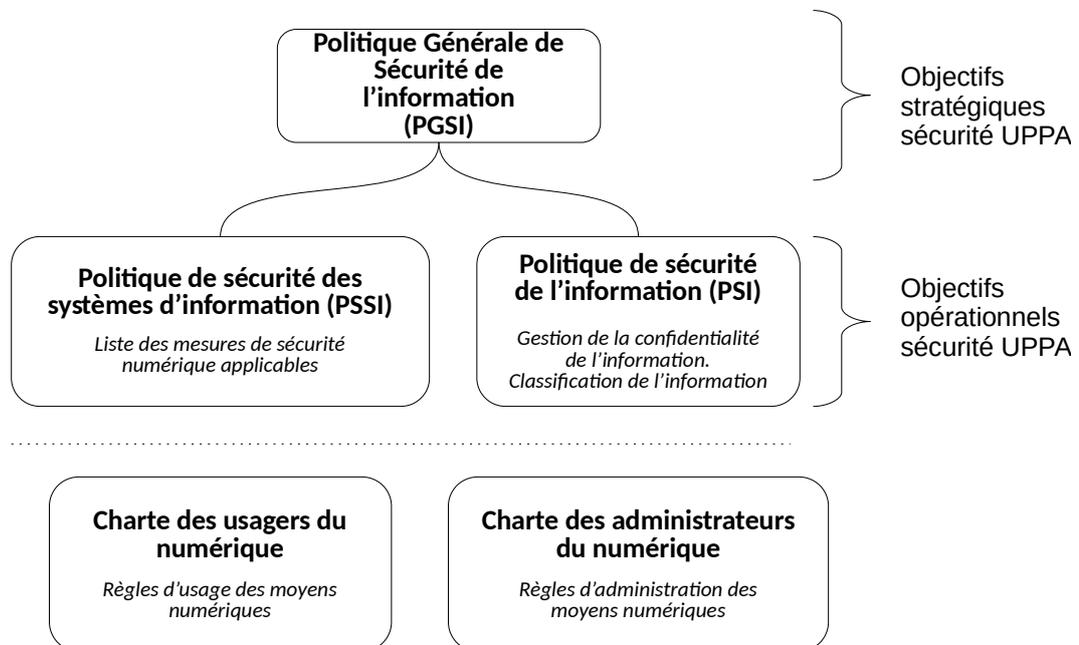
1. DOMAINE D'APPLICATION

1.1. Contexte

L'université de Pau et des pays de l'Adour (UPPA) fait partie des universités françaises labellisées I-SITE, Initiatives Science, Innovation, Territoires, Économie. À ce titre, elle est amenée à participer à des projets portés par le consortium UPPA, INRA, Inria, CNRS (Label I-SITE).

Pluridisciplinaire, ses activités se déploient sur les sites de Pau, Bayonne, Anglet, Mont-de-Marsan, Tarbes et Saint-Pée-sur-Nivelle.. L'UPPA accueille près de 13000 étudiants, sa recherche se déploie notamment dans 19 unités de recherche, plus de 30 chaires d'expertises et 10 laboratoires communs en partenariat avec des organismes de recherche (CNRS, INRAE, Inria) et des partenaires publics ou privés.

Cette politique de sécurité des systèmes d'information décline la politique générale de sécurité de l'information de l'UPPA en mesures de sécurité. Elle décrit les spécificités de l'UPPA dans la mise en application de la politique de sécurité des systèmes d'information de l'État (PSSIe) selon le schéma :



1.2. Périmètre

La PSSI de l'UPPA s'applique à l'ensemble de ses Systèmes d'Information (SI), c'est-à-dire à tous les processus métiers et leurs informations ainsi qu'à toutes les fonctions de support nécessaires à la bonne gestion de ces processus, quelle que soit leur localisation.

Les SI couverts par la présente PSSI sont issus des trois missions de l'UPPA et s'articulent autour de :

- la formation et la vie universitaire ;
- la recherche et l'innovation ;
- le pilotage de l'établissement.

1.3. Les besoins en sécurité de l'UPPA

Les SI de l'université sont indispensables pour les activités d'enseignement, de recherche et de pilotage/gestion. Ils sont susceptibles de présenter des vulnérabilités qui pourraient être exploitées par des activités de cybermalveillance.

Cela pourrait avoir des conséquences sur la disponibilité, l'intégrité et la confidentialité des informations de l'UPPA.

Afin de répondre aux besoins de sécurité de l'ensemble des missions de l'établissement, il est nécessaire de se protéger des menaces internes et externes. Des mesures de sécurité adaptées sont définies et mises en œuvre afin d'amener les risques à un niveau acceptable.

2. MISE EN APPLICATION DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

Afin de sécuriser ses SI, l'UPPA, s'attache à mettre en œuvre un ensemble de règles de sécurité répondant à la démarche de pilotage par les objectifs de sécurité de l'information en prenant en compte les règles générales, émanant de la PSSI de l'État.

2.1. Pilotage par les objectifs de sécurité des systèmes d'information

Pour assurer la sécurité de ses SI, l'UPPA s'appuie sur

- l'alignement de la sécurité du numérique (SécNum) sur la stratégie de l'établissement,
- l'analyse de risque de ses activités sur la base d'un processus itératif,
- l'homologation de sécurité issue du référentiel général de sécurité (RGS),
- la mise en œuvre des mesures de sécurité identifiées.

Ces règles viennent compléter, amender ou renvoyer vers, les règles de la PSSIe, faisant partie du cadre de référence de la sécurité de l'information de l'UPPA.

2.2. Le cadre de référence de la sécurité l'information pour l'UPPA

2.2.1. Guide d'hygiène informatique de l'ANSSI

Le guide d'hygiène informatique de l'ANSSI est un document qui présente les 40 règles d'hygiène informatique indispensables mais non exhaustives. Elles constituent cependant le socle minimum des règles à respecter pour protéger les informations de l'établissement. Elles décrivent des mesures concrètes de sécurisation, notamment à destination des équipes du pôle numérique de l'UPPA.

La mise en œuvre de ces règles est un préalable au déploiement des activités de sécurité du numérique.

2.2.2. La Politique de Sécurité des Systèmes d'Information de l'État

En cas d'absence de règles et mesures de sécurité spécifiques, l'UPPA s'attachera à respecter le socle de sécurité de l'État décrit sur le site de l'agence nationale de la sécurité des systèmes d'information (ANSSI), permettant ainsi de s'appuyer sur un niveau de sécurité suffisant pour se protéger de la plupart des risques numériques usuels et non ciblés.

La PSSIe, portée par la circulaire du Premier ministre n° 5725/SG du 17 juillet 2014, est un ensemble de règles de protection applicables aux systèmes d'information de l'État .

Ces règles sont réparties en 7 grandes catégories :

- Gouvernance,
- Maîtrise des risques,
- Évaluation,
- Maîtrise des Systèmes,
- Protection des Systèmes,
- Gestion des Incidents,
- Continuité d'activité.

2.2.3. Politique Générale de Sécurité de l'Information

La PGSI décrit la vision stratégique des risques pesants sur l'information dans le cadre des grandes missions de l'UPPA. Elle constitue le document fondateur du cadre de référence de la sécurité de l'information.

Elle permet, au travers de la formulation d'un ensemble de grands principes, d'introduire les règles opérationnelles :

- Principes de Gouvernance de la sécurité de l'information
 - Principe directeur de la sécurité de l'information
 - Principe d'organisation pour la sécurité de l'information
 - Principe de pilotage de la sécurité de l'information
- Principes de sécurité de l'information
 - Principe de protection de l'information
 - Principe de maîtrise des habilitations et du contrôle des accès
 - Principe de sensibilisation et formation des utilisateurs
 - Principe de protection des SI
 - Principe de sécurité de l'information, y compris dans les relations avec les tiers
 - Principe de continuité d'activité
 - Principe de gestion des incidents de sécurité de l'information

2.2.4. La Politique de Sécurité de l'Information

La sécurité de l'information se base sur :

- Une mise en contexte réglementaire, définissant notamment les cadres relatifs aux informations du potentiel scientifique et technique de la nation et à la protection des données à caractère personnel,
- La caractérisation de l'information au travers de sa définition et de sa classification.

Cette vision permet une bonne mise en application des règles relatives au traitement de l'information.

2.2.5. Le règlement intérieur et les chartes

Le règlement intérieur est opposable à tous les agents et usagers. De plus, des règles spécifiques sont formulées dans deux chartes :

- l'une à destination des usagers du numérique, ainsi qu'à ceux disposant à titre dérogatoire des droits administrateur de leur poste,
- l'autre à destination des administrateurs du numérique, disposant de droits d'accès privilégiés aux actifs des SI de l'UPPA et devant respecter un ensemble d'obligations supplémentaires et de bonnes pratiques.

2.3. Accès aux mesures de sécurité

Les mesures de sécurité de la PSSI sont consultables par les agents depuis le site institutionnel à la

rubrique « Recueil des Actes Administratifs (RAA) ».

Elles sont présentées sous la forme d'un tableau dans lequel les spécificités de l'établissement vis-à-vis de la PSSle sont matérialisées par les indicateurs suivants :

- acceptée,
- refusée,
- amendée,
- ajoutée (issue des besoins spécifiques de l'UPPA).