école normale supérieure paris-saclay

Le conseil d'administration
de l'ENS Paris-Saclay

Séance du 12 décembre 2025

Délibération 2025-35

Point de l'ordre du jour : IV 4.5

Objet : Politique de sécurité des systèmes d'information (PSSI) 2026-2028

Vu le code de l'Education,
Vu le décret n°2011-21 du 5 janvier 2011 relatif à l'École normale supérieure Paris-Saclay ;
Vu la circulaire du Premier Ministre n° 5725/SG du 17 juillet 2014 relative à la politique de sécurité des systèmes d'information de l'Etat (PSSIE) ;
Vu le règlement intérieur de l'École normale supérieure Paris-Saclay.
Considérant que l'ENS Paris-Saclay doit se doter d'une Politique de Sécurité des Systèmes d'Information (PSSI) ;

Vote unique :

Le conseil d'administration approuve la Politique de Sécurité des Systèmes d'Information (PSSI) pour la période 2026-2028 telle que présentée dans le document annexé à la présente délibération.

Nombres de votants : 25

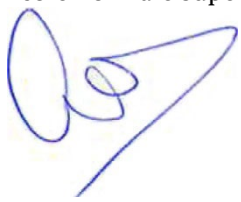
Pour : 25

Contre : 0

Abstention : 0

Fait à Gif-sur-Yvette, le 12/12/2025.

Pour extrait conforme,
La Présidente de l'École normale supérieure Paris-Saclay



Nathalie CARRASCO

Pièce jointe : PSSI 2026-2028

Classée au registre des délibérations sous la référence :	Modalités de recours contre la présente délibération :
CA – 12/12/2025 - D.2025-35	En application de l'article R.421-1 et suivants du code de justice administrative, la présente délibération pourra faire l'objet, dans

ENS Paris-Saclay www.ens-paris-saclay.fr 4 avenue des sciences CS30008 91192 Gif-sur-Yvette Cedex

Publiée sur le site internet de l'ENS Paris-Saclay le :	un délai de deux mois à compter de sa notification et /ou de sa publication, d'un recours gracieux auprès de la Présidente de l'ENS Paris-Saclay, et/ou d'un recours pour excès de pouvoir devant le Tribunal administratif de Versailles.

ENS Paris-Saclay www.ens-paris-saclay.fr 4 avenue des sciences CS30008 91192 Gif-sur-Yvette Cedex

Politique de sécurité des systèmes d'information 2026 -2028

École normale supérieure Paris-Saclay

Identification du document

Date de création/modification : 02/04/2024
Date d'application : 01/01/2026
Version finale

Le présent document constitue la version synthétique de la Politique de sécurité des systèmes d'information (PSSI) de l'ENS Paris-Saclay.
Il établit les principes fondamentaux de sécurité, les acteurs clés, le périmètre, et les références réglementaires.
Il ne comprend pas, à ce stade, la déclinaison détaillée des objectifs en exigences techniques, indicateurs de conformité, ou matrices de responsabilité.
Ces éléments seront précisés dans les documents de mise en œuvre associés à chaque objectif, sur la base de la PSSIE et de la norme ISO/IEC 27002.

Table des matières

1. Objectif de la PSSI

La Politique de sécurité des systèmes d'Information (PSSI) de l'ENS Paris-Saclay utilise comme référentiel la PSSIE (c'est-à-dire la Politique de Sécurité des Systèmes d'Information de l'État) ainsi que les meilleures pratiques internationales telles que celles de la norme ISO/IEC 27001. Elle s'inscrit également dans le respect du Règlement général sur la protection des données (RGPD – UE 2016/679), du Référentiel Général de Sécurité (RGS), et des lignes directrices de la norme ISO/IEC 27002. Ces référentiels édictent un ensemble d'objectifs et de règles destinés à assurer la protection des systèmes d'information.

La PSSIE établit les principes stratégiques et décline les règles de leur mise en œuvre. Parmi les principes retenus, il faut souligner les dispositions suivantes :

- Les moyens humains et financiers consacrés à la SSI doivent être planifiés, quantifiés et identifiés au sein des ressources globales des systèmes d'information, et réévalués régulièrement pour répondre aux nouvelles menaces ;
- Les opérations de gestion et d'administration des systèmes d'information doivent être tracées, contrôlées et auditées régulièrement ;
- Chaque agent doit être informé de ses droits et devoirs, mais également être formé et sensibilisé à la cybersécurité ;
- Les informations considérées comme sensibles, en raison de leurs besoins en confidentialité, intégrité ou disponibilité, doivent être hébergées sur le territoire national; leur sensibilité étant appréciée selon une grille de classification interne intégrée aux pratiques de gestion documentaire et de gouvernance des données ;
- Chaque établissement devait se doter d'une PSSI au 1er janvier 2015 et s'assurer de l'application des mesures de la PSSIE dans un délai de trois ans à compter de sa publication.

Ce document (PSSI de l'ENS Paris-Saclay) définit les exigences techniques et organisationnelles de la sécurité des systèmes d'information de l'ENS Paris-Saclay, et répond aux principes directeurs suivants :

- L'ENS Paris-Saclay dimensionne et met en œuvre tous les moyens humains et financiers afin de répondre aux enjeux de la présente PSSI ; le pilotage global étant assuré par le RSSI, qui est responsable de la déclinaison opérationnelle, du suivi des plans d'action SSI, et du reporting auprès de la direction ;
- Des moyens d'authentification, proportionnels aux besoins de sécurité et suffisamment robustes, doivent être déployés par l'ENS Paris-Saclay afin de gérer les accès aux ressources par les parties prenantes du SI ; les mécanismes privilégiés incluent l'authentification multifacteur (MFA), l'authentification unique (SSO) et une gestion centralisée des habilitations ;
- Afin de protéger son système d'information, l'ENS Paris-Saclay doit mettre en œuvre les mesures techniques de protection nécessaires ;
- Toute opération liée à la gestion et à l'administration du système doit être tracée, contrôlée et auditée de manière régulière pour garantir la conformité et la sécurité ;

- Chaque utilisateur des ressources informatiques mises à sa disposition par l'ENS Paris-Saclay doit être sensibilisé et informé de ses droits et devoirs via des formations régulières et des simulations de cyberattaques ;
- Les administrateurs doivent adopter les règles de sécurité informatique dans le cadre de leurs fonctions, et leur accès doit être régulièrement réévalué ;
- Avant toute mise en œuvre d'un système, ce dernier doit être documenté, et une analyse de risques doit être conduite par le CSSI (avec le support du RSSI en cas de besoin) afin de traiter les risques pesant sur celui-ci. Ce principe constitue une action préventive et s'inscrit dans une démarche d'amélioration continue ;
- L'usage des services cloud est encadré afin de garantir la maîtrise des données, la localisation des traitements, la sécurité des accès et la réversibilité des services. Lorsque la sensibilité des données ou des traitements le justifie, l'ENS Paris-Saclay privilégie des solutions qualifiées SecNumCloud ou conformes aux recommandations de l'ANSSI ;
- Afin d'éviter une diffusion fortuite à des tiers non autorisés, il est important de mentionner sur un document son niveau de confidentialité. Le rédacteur du document en a la charge ;
- La sécurité des systèmes d'information (SSI) concerne tous les personnels de l'ENS Paris-Saclay et doit être intégrée dans toutes les activités quotidiennes de l'établissement.

Ces principes résument les objectifs à atteindre pour renforcer le niveau de sécurité de l'ENS Paris-Saclay.
Leur déclinaison sous forme de procédures, de mesures techniques et d'indicateurs de conformité fera l'objet de documents de mise en œuvre associés à chaque objectif stratégique.
La mise en œuvre s'inscrit dans une trajectoire pluriannuelle, structurée sur une période de trois ans, avec des revues annuelles et des réévaluations semestrielles portant sur les risques, les écarts identifiés lors des audits, et les indicateurs de conformité.
Cette approche garantit la pertinence et l'efficacité du dispositif face aux nouvelles menaces et aux évolutions technologiques.

2. Périmètre d'application de la PSSI

Le Système d'information inclut l'ensemble des informations, processus et échanges informationnels, entre entités. Le système d'information comprend l'ensemble des données, des processus, des équipements, des flux et des échanges permettant aux entités de l'ENS Paris-Saclay d'exercer leurs missions dans le cadre des services qu'elles assurent.

Toutes les entités ainsi que les prestataires et les services externalisés, s'inscrivent dans ce périmètre et sont tenus de se conformer à la présente Politique de sécurité des systèmes d'Information (PSSI).

La sécurité des systèmes d'information (SSI) couvre l'ensemble des composantes du système d'information de l'ENS Paris-Saclay, avec toute la diversité que cela implique en termes d'usages, de lieux d'utilisation, de méthodes d'accès et de types d'utilisateurs. Le périmètre de la SSI inclut notamment :

- Le système informatique de gestion ;
- Les applications institutionnelles (messagerie, intranet, sites web, stockage, sauvegarde…) ainsi que les applications propres aux directions, laboratoires et services (applications scientifiques, outils de traitement de données, bureautique, gestion de la scolarité, etc.) ;
- Les systèmes s'appuyant sur des ressources informatiques sans en relever directement (ToIP/VoIP, visioconférence, vidéosurveillance, contrôle d'accès physique…) ;
- Les interconnexions et échanges avec les partenaires institutionnels ou scientifiques (CNRS, Université Paris-Saclay, CentraleSupélec, etc.) ;
- Les environnements cloud, les infrastructures externalisées et les services numériques tiers.

La SSI s'applique également aux personnels de l'établissement en situation de mobilité, notamment :

- En mission ou déplacement professionnel ;
- En télétravail ;
- Utilisant des terminaux personnels pour accéder au système d'information (BYOD – Bring Your Own Device).

Les laboratoires de l'ENS Paris-Saclay comportant des zones à régime restrictif (ZRR) sont soumis au dispositif national de protection du potentiel scientifique et technique (PPST), piloté par le Haut fonctionnaire de défense et de sécurité (HFDS). À ce titre, ils doivent :

- Réaliser un inventaire et une analyse des risques associés ;
- Élaborer et mettre en œuvre une PSSI spécifique au laboratoire, pouvant s'appuyer sur la présente politique ou sur les politiques de tutelles (ex. : CNRS, INRAE…) ;
- Mettre en place les mesures de protection nécessaires pour prévenir les risques d'ingérence et de captation d'informations par des acteurs étrangers.

La présente politique est révisée au minimum tous les trois ans, ou plus fréquemment dans les cas suivants :

- Un contrôle, résultats d'audits ou d'analyses de risques ;
- Un changement important, en termes d'organisation, évolution technologique ou de réglementations ;
- Un incident important survenu sur le système d'information.

Elle est validée par l'**Autorité qualifiée pour la sécurité des systèmes d'information (AQSSI)**, rôle dévolu à la présidente de l'ENS Paris-Saclay. Elle entre en vigueur à compter de sa publication officielle. Une notification formelle est transmise à l'ensemble des personnels et partenaires concernés afin d'assurer la prise de connaissance et l'adhésion à la politique.

Toute exception à une règle de la présente politique doit faire l'objet d'une dérogation, justifiée par le demandeur, analysée par le RSSI, évaluée par une analyse de risques détaillée et validée par l'AQSSI. Les risques liés à la non-application d'une règle doivent être pleinement identifiés par le demandeur, documentés, et assortis de mesures compensatoires adaptées.

Toute entité de l'ENS Paris-Saclay applique la présente PSSI comme référence. Toutefois, lorsque des besoins particuliers l'exigent (ex. : présence d'une ZRR, exigences spécifiques d'une tutelle, projets à enjeux), l'entité concernée peut formaliser une PSSI propre. Cette déclinaison locale doit être :

- Cohérente avec les principes de la PSSI de l'ENS Paris-Saclay ;
- Validée par la direction de l'entité avec l'appui du RSSI ;
- Non substitutive à la politique-cadre, sauf disposition contractuelle expresse ou réglementation contraignante.

2.1 Cadre juridique

2.1.1 La loi Informatique et Libertés et le règlement général sur la protection des données (RGPD)

Conformément à la loi « Informatique et Libertés » du 6 janvier 1978 modifiée et au Règlement (UE) 2016/679 du 27 avril 2016 (applicable depuis le 25 mai 2018), les personnes sont protégées contre tout traitement abusif de données à caractère personnel les concernant. Cette protection s'applique dans l'ensemble des pays de l'Union européenne.

Selon l'article 6 de la loi n°78-17 du 6 janvier 1978 :

« Les traitements ne peuvent porter que sur des données collectées et traitées de manière loyale et licite, pour des finalités déterminées, explicites et légitimes, adéquates, pertinentes et non excessives au regard de leur finalité, exactes, complètes et tenues à jour, et qui ne doivent pas être conservées plus que la durée nécessaire aux finalités pour lesquelles elles ont été collectées. »

L'article 34 impose des mesures de sécurité pour protéger les données, tandis que les articles 38 à 43 précisent les droits des personnes (accès, rectification, opposition, etc.) vis-à-vis des traitements.

Le **Délégué à la protection des données (DPD)** de l'ENS Paris-Saclay coordonne la tenue à jour du registre des traitements de données à caractère personnel. Chaque responsable de traitement est tenu de lui signaler tout nouveau traitement, afin qu'il soit identifié, consigné et audité si nécessaire. Dans les unités mixtes, le DPD de l'ENS Paris-Saclay ou celui de l'organisme de tutelle peut être indifféremment contacté.

2.1.2 La Loi pour la confiance dans l'économie numérique (LCEN)

La loi n°2004-575 du 21 juin 2004 impose aux fournisseurs d'accès et aux hébergeurs de services en ligne la conservation des journaux techniques permettant de tracer l'activité des utilisateurs, pendant une durée légale. En cas d'incident, ces journaux doivent permettre d'identifier un utilisateur à partir d'une adresse IP ou d'un identifiant unique, sur requête judiciaire.

Conformément à la LCEN, tout signalement de contenu illicite hébergé sur une infrastructure dont l'adresse IP appartient à l'ENS Paris-Saclay doit entraîner :

- Son retrait immédiat,
- Ainsi qu'un signalement au RSSI.

2.1.3 Le respect de la propriété intellectuelle

La loi protège les auteurs contre l'appropriation ou la reproduction non autorisée de leurs œuvres littéraires, scientifiques, artistiques ou logicielles. Le téléchargement ou la mise à disposition d'œuvres protégées depuis les équipements connectés au réseau de l'ENS Paris-Saclay est interdit.

Le code de la propriété intellectuelle couvre notamment :

- Les œuvres de l'esprit,
- Les logiciels et bases de données,
- Les marques, dessins et modèles.

Tout usage de logiciel ou de document protégé par copyright doit respecter les termes des licences applicables.

2.1.4 Le Référentiel général de sécurité (RGS)

Le **RGS** encadre les échanges électroniques entre usagers et autorités administratives, ou entre autorités. Il est défini par le décret n°2010-112 du 2 février 2010, dans sa version 2.0 approuvée par arrêté du 13 juin 2014, avec des mesures transitoires étendues par arrêté du 10 juin 2015. Il s'applique depuis le 1er juillet 2014.

Ce référentiel définit les exigences de sécurité applicables à :

- L'usage de produits de sécurité (ex. : certificats, horodatage),
- Les services de certification électronique,
- Le recours à des prestataires d'audit ou de services cloud.

Les agents de l'ENS Paris-Saclay confrontés à ces exigences doivent se rapprocher de la DSI ou des correspondants informatiques de leur structure.

2.1.5 La protection du potentiel scientifique et technique (PPST)

Le dispositif **PPST**, instauré par le décret n°2011-1425 du 2 novembre 2011, organise la protection de savoirs ou technologies sensibles contre la prédation étrangère, dans un objectif de sécurité économique et de lutte contre la prolifération.

Il repose notamment sur la mise en œuvre de **Zones à régime restrictif (ZRR)** : zones dont l'accès (y compris numérique) est strictement réglementé. Tout accès à une ZRR doit être autorisé par le directeur du laboratoire concerné, en cohérence avec la présente PSSI.

Le directeur de laboratoire doit veiller à doter l'unité d'une PSSI propre, s'inspirant au besoin de celle de l'ENS Paris-Saclay ou d'une tutelle.

Le Fonctionnaire de sécurité et de défense (FSD), et son ou sa suppléante, représentent le relais local du haut fonctionnaire de défense et de sécurité (HFDS) du ministère. Ils assurent le lien avec la présidence de l'établissement et veillent à l'application des consignes nationales en matière de sécurité scientifique.

La PSSI et la PPST sont étroitement liées, toutes deux placées sous la responsabilité de la présidence de l'ENS Paris-Saclay. Leur articulation permet de répondre aux exigences croissantes de protection du potentiel académique et scientifique.

2.1.6 La charte d'usage du système d'information

La charte d'usage du numérique définit les conditions d'utilisation des ressources informatiques mises à disposition au sein de l'ENS Paris-Saclay. Elle fait partie intégrante du règlement intérieur et s'impose à tout personnel, étudiant ou intervenant ayant accès au système d'information.

2.2 Besoins de sécurité

La sécurité du système d'information repose sur les critères fondamentaux suivants :

- **Confidentialité** :

« La confidentialité est la propriété qu'une information ne soit ni disponible ni divulguée à des entités (personnes, unités ou processus) non autorisées » *(ISO/CEI 74S8-2)*

- **Disponibilité** :

Propriété d'accessibilité, au moment voulu, des données et des services par les utilisateurs autorisés.

- **Intégrité** :

« L'intégrité est la prévention de la modification non autorisée de l'information » *(ISO/CEI 74S8-2)*

Ces besoins de sécurité s'appliquent à l'ensemble des ressources du système d'information (postes de travail, serveurs, réseaux, applications, équipements nomades, services cloud, etc.) ainsi qu'aux données traitées, stockées ou transmises par ces ressources.

Il est essentiel de procéder à une classification des données selon leur nature (administrative, scientifique, personnelle, stratégique, réglementaire…), leur sensibilité, et les impacts potentiels d'une compromission.

Cette classification permet d'identifier le niveau de protection requis, selon les critères de confidentialité, intégrité et disponibilité. Elle constitue un prérequis à la mise en œuvre des mesures organisationnelles et techniques appropriées.

La protection des données doit également intégrer des dispositifs de prévention des fuites d'information (Data Loss Prevention – DLP), en particulier pour :

- Les échanges externes,
- Les supports amovibles,
- Et les usages en mobilité.

2.3 Menaces

Afin de mettre en place les moyens de sécurité adéquats, il est nécessaire d'identifier les menaces susceptibles d'affecter le système d'information, en s'appuyant sur une méthode de gestion des risques reconnue, telle que la méthode EBIOS Risk Manager (Expression des Besoins et Identification des Objectifs de Sécurité – version ANSSI).

Les menaces peuvent être regroupées selon leur nature et leur cible :

- **Les attaques ciblant directement le système d'information** :
  Vol ou divulgation non autorisée de données, compromission des comptes, modification malveillante d'informations, sabotage ou déni de service (DDoS) rendant les services indisponibles.
- **Les attaques visant les ressources informatiques** :
  Vol ou détournement de matériel, utilisation illicite des ressources (minage de cryptomonnaies, stockage non autorisé…), altération physique ou logique des systèmes, diffusion de logiciels malveillants (malwares, ransomwares, vers…).
- **Les événements accidentels ou environnementaux** :
  Sinistres naturels (incendie, inondation), défaillances matérielles, erreurs humaines, altération involontaire des données ou des ressources.
- **Les usages non maîtrisés ou les négligences internes** :
  Défaut de formation, comportements à risque, mauvais paramétrage, absence de suivi des droits d'accès, réutilisation de mots de passe, configuration inadéquate de services cloud.

Pour chaque menace identifiée, une évaluation du risque doit être réalisée, combinant :

- Sa vraisemblance,
- Et son impact potentiel.

Cette analyse doit également prendre en compte :

- Les facteurs aggravants (ex. : exposition sur Internet, manque de supervision, absence de correctifs),
- Ainsi que les vulnérabilités internes exploitables.

L'objectif est de déterminer les niveaux de risque résiduel, afin de prioriser les mesures de sécurité à mettre en œuvre.

2.4 Sensibilisation des usagers aux risques numériques

La majorité des attaques numériques impliquent aujourd'hui une action humaine : clic sur un lien piégé, réponse à un message frauduleux, installation involontaire d'un logiciel malveillant… Ces vecteurs sont devenus les plus fréquents, dépassant largement les vulnérabilités purement techniques.

Les campagnes de hameçonnage (phishing), l'usurpation d'identité ou l'ingénierie sociale exploitent des canaux variés : messagerie professionnelle, messagerie personnelle, réseaux sociaux, SMS, ou appels téléphoniques. Elles visent à obtenir des identifiants, des accès à des systèmes sensibles, ou à déclencher une action préjudiciable.

Les protections techniques restent indispensables (pare-feu, antivirus, filtrage DNS, authentification multifacteur), mais elles ne suffisent pas à neutraliser ces attaques si les utilisateurs ne sont pas correctement informés, formés et accompagnés.

La politique de sécurité de l'ENS Paris-Saclay intègre une stratégie active de sensibilisation, basée sur :

- Des campagnes régulières d'information et de rappel des bons réflexes ;
- Des sessions de formation dédiées (nouveaux arrivants, chercheurs, fonctions sensibles…) ;
- Des simulations réalistes d'attaques (phishing simulé, usurpation ciblée) ;
- Une veille active sur les nouvelles méthodes d'attaque.

Chaque personnel, enseignant, étudiant ou doctorant doit être capable de :

- Reconnaître un message frauduleux ou suspect (phishing, spear phishing, escroquerie par usurpation) ;
- Appliquer les bons réflexes : ne pas cliquer, ne pas transmettre d'informations sensibles, signaler immédiatement ;
- Utiliser des mots de passe robustes, uniques, et activer l'authentification multifacteur dès que possible ;
- Maintenir ses outils à jour, limiter les droits des applications, et se méfier des connexions inconnues.

Les attaques par IA générative représentent un nouveau palier : elles permettent de produire des messages, des voix, voire des vidéos ultra-crédibles, ciblées et personnalisées à partir des données publiques (profil LinkedIn, publications scientifiques, conférences, etc.).

L'ENS Paris-Saclay intègre désormais ces risques dans ses actions de sensibilisation, avec une attention particulière pour les profils exposés (chercheurs en ZRR, décideurs, administrateurs).

Il est essentiel de faire évoluer les méthodes de sensibilisation au même rythme que les menaces : le facteur humain reste la première ligne de défense.

2.5 Gouvernance de la SSI

Au sein de l'ENS Paris-Saclay, la responsabilité générale de la sécurité des systèmes d'information relève de la présidente de l'établissement, en tant qu'autorité qualifiée pour la sécurité des systèmes d'information (AQSSI).

Elle est assistée par :

- Le Fonctionnaire de sécurité et de défense (FSD) et son ou sa suppléant·e dans le cadre du dispositif PPST (Protection du Potentiel Scientifique et Technique),
- Et par le responsable de la sécurité des systèmes d'information (RSSI) pour la mise en œuvre de la PSSI.

La PSSI de l'ENS Paris-Saclay s'inscrit dans les orientations de l'**ANSSI**, via :

- La PSSIE,
- Et les recommandations sectorielles.

Pour les entités impliquées dans la recherche, ces orientations sont également portées par le haut fonctionnaire de défense et de sécurité (HFDS) du ministère de l'enseignement supérieur et de la recherche, avec l'appui d'un FSSI (Fonctionnaire de sécurité des systèmes d'information).

Le pilotage opérationnel de la sécurité est assuré par le RSSI, qui :

- Anime le réseau des correspondants SSI (CSSI) dans les directions, laboratoires ou services,
- Coordonne la déclinaison locale de la politique de sécurité,
- Suit le plan d'action SSI,
- Gère les incidents de sécurité,
- Coordonne les audits internes,
- Et assure le reporting régulier auprès de l'AQSSI.

Chaque direction ou laboratoire est responsable de la sécurité dans son périmètre.

Elle doit désigner un correspondant SSI (CSSI) chargé de :

- Relayer la politique SSI locale,
- Sensibiliser les utilisateurs,
- Participer aux analyses de risques,
- Faire remonter les incidents au RSSI,
- Contribuer à la mise en conformité de l'entité.

La DSI (Direction des systèmes d'information), et si besoin le service de gestion des accès et des infrastructures, assurent la mise en œuvre des moyens techniques, notamment pour :

- Le contrôle des flux,
- La gestion des accès,
- Et la protection des ressources numériques.

Chaque entité doit adapter les exigences de la PSSI à son contexte, ses risques spécifiques et ses ressources.

Les acteurs SSI doivent être informés de leurs rôles et obligations, y compris en matière de devoir de réserve ou secret professionnel, selon les cas.

L'implication de l'ensemble des personnels – direction, enseignants, chercheurs, techniciens et administratifs – est déterminante.

La SSI repose sur une démarche collective, dans une logique d'amélioration continue.

Un plan d'action local, avec calendrier de mise en conformité, doit être défini dans chaque entité pour garantir l'application effective de la présente politique.

2.6 Coordination avec les autres tutelles

Cas des unités mixtes ou hébergées

Le système d'information des unités de recherche mixtes ou hébergées est également concerné par la PSSI de l'ENS Paris-Saclay, sauf dispositions contraires prévues explicitement dans les conventions de partenariat (ex. CNRS, Inria, universités partenaires).

Les contrats de tutelle (ex. contrat quadriennal) doivent :

- Intégrer les exigences SSI,
- Clarifier les responsabilités de chaque acteur,
- Et désigner la PSSI de référence applicable à l'unité (UMR, UMI, unité propre...).

Le directeur de l'unité, en tant que responsable SSI dans son périmètre, doit :

- S'assurer que les documents de sécurité de son unité (PSSI locale, charte informatique, politique de gestion des journaux, etc.) sont compatibles avec les exigences des différentes tutelles (ENS Paris-Saclay, CNRS, Inria, etc.) ;
- Désigner un Correspondant Sécurité des Systèmes d'Information (CSSI), qui agit comme interface fonctionnelle entre les tutelles.

Le CSSI fait partie des chaînes fonctionnelles SSI de chaque tutelle, et assure :

- La coordination des informations,
- Le suivi des alertes,
- Et la transmission des actions correctives

En cas d'incident :

- Le traitement est assuré par la tutelle identifiée comme responsable opérationnelle,
- En coordination avec le CSSI,
- Et avec l'appui du RSSI de l'ENS Paris-Saclay, qui veille à l'information des autres partenaires et à la concertation sur les suites (dépôt de plainte, notification CNIL, etc.).

Les procédures de gestion des incidents doivent être :

- Partagées,
- Documentées,
- Et alignées avec les meilleures pratiques nationales et internationales (ANSSI, CERT-FR, ISO/IEC 27035...).

3. Mise en œuvre opérationnelle de la PSSI

La Politique de sécurité des systèmes d'information (PSSI) de l'ENS Paris-Saclay s'appuie sur les 13 objectifs stratégiques définis par la politique de sécurité des systèmes d'information de l'état (PSSIE), en cohérence avec la norme ISO/IEC 27002. Ces objectifs couvrent l'ensemble des domaines essentiels à la sécurité du système d'information :

- **O1** : Politique, organisation, gouvernance
- **O2** : Ressources humaines
- **O3** : Gestion des biens
- **O4** : Intégration de la SSI dans le cycle de vie des SI
- **O5** : Sécurité physique
- **O6** : Sécurité des réseaux
- **O7** : Architecture des SI
- **O8** : Exploitation des SI
- **OG** : Sécurité du poste de travail
- **O10** : Sécurité du développement des systèmes
- **O11** : Traitement des incidents
- **O12** : Continuité d'activité
- **O13** : Conformité, audit, inspection, contrôle

La mise en œuvre de ces objectifs repose sur une déclinaison opérationnelle structurée selon les principes suivants :

- Traduction des objectifs en exigences concrètes, sous la forme de règles, procédures, chartes ou guides applicables à l'échelle de l'établissement ;
- Pilotage central par le RSSI, responsable de la coordination des actions, de l'animation du réseau des Correspondants SSI (CSSI), et de l'appui aux entités ;
- Identification et suivi d'indicateurs de conformité, permettant de mesurer l'application des exigences, d'identifier les écarts et de prioriser les actions correctrices ;
- Suivi régulier et itératif, avec des revues de conformité annuelles et des réévaluations semestrielles des priorités en fonction des menaces, des évolutions réglementaires, des audits et des incidents constatés ;
- Intégration des exigences de sécurité à la gouvernance numérique, aux projets informatiques, aux marchés publics et aux procédures de gestion des accès.

Le RSSI assurera la tenue d'un tableau de bord SSI consolidé, recensant pour chaque objectif les actions engagées, leur état d'avancement, les responsables associés, les ressources mobilisées, et les indicateurs suivis. Ce tableau de bord permet un reporting régulier auprès de la direction et des instances compétentes.

Des documents de mise en œuvre spécifiques viendront compléter la présente PSSI. Ils préciseront pour chaque objectif les modalités d'application, les responsabilités, les ressources et les échéances associées. Ces documents seront mis à disposition des entités et actualisés régulièrement.

Cette approche vise à inscrire la sécurité dans une démarche d'amélioration continue, portée par une gouvernance active, une coordination transverse, et une progression pluriannuelle de la maturité SSI.

4. Glossaire

AQSSI – *Autorité qualifiée pour la sécurité des systèmes d'Information*
Personne ayant autorité pour valider la politique de sécurité d'un organisme. À l'ENS Paris-Saclay, ce rôle est assumé par la présidence.

BYOD – *Bring Your Own Device*
Utilisation d'un équipement personnel (ordinateur, téléphone…) pour accéder au système d'information de l'établissement.

CSSI – *Correspondant sécurité des systèmes d'information*
Relai local du RSSI dans un laboratoire, un service ou une direction. Il contribue à la sensibilisation, au suivi des incidents et à la mise en œuvre des mesures de sécurité.

DPD – *Délégué à la Protection des Données*
Personne désignée pour veiller à la conformité des traitements de données personnelles au RGPD.

DSI – *Direction des Systèmes d'Information*
Service en charge de l'architecture, du fonctionnement et de la sécurité technique du système d'information.

FSD – *Fonctionnaire de Sécurité et de Défense*
Personne chargée de mettre en œuvre localement les consignes nationales de sécurité dans le cadre du PPST, en lien avec le HFDS.

HFDS – *Haut Fonctionnaire de Défense et de Sécurité*
Représentant du ministère chargé de coordonner la politique de sécurité, notamment dans le cadre du dispositif PPST.

ISO/IEC 27001 / 27002
Normes internationales établissant les bonnes pratiques pour la gestion de la sécurité de l'information (27001 = exigences ; 27002 = mesures de sécurité recommandées).

PSSI – *Politique de Sécurité des Systèmes d'Information*
Document définissant les objectifs, principes, responsabilités et exigences en matière de sécurité numérique d'un organisme.

PSSIE – *Politique de Sécurité des Systèmes d'Information de l'État*
Cadre de référence établi par l'ANSSI pour les organismes publics, décrivant 13 objectifs stratégiques de sécurité.

PPST – *Protection du Potentiel Scientifique et Technique*
Dispositif réglementaire visant à protéger les savoirs sensibles contre la prédation étrangère, notamment dans les ZRR.

RGPD – *Règlement Général sur la Protection des Données*
Règlement européen (2016/679) encadrant la protection des données à caractère personnel.

RSSI – *Responsable de la Sécurité des Systèmes d'Information*
Personne chargée de piloter la SSI d'un établissement, de coordonner les actions de sécurité, de suivre les incidents et d'animer le réseau des CSSI.

RGS – *Référentiel Général de Sécurité*
Référentiel défini par l'État français pour sécuriser les échanges électroniques entre administrations, usagers et partenaires.

SSI – *Sécurité des Systèmes d'Information*
Ensemble des mesures destinées à assurer la **confidentialité**, l'**intégrité**, la **disponibilité**, et la **traçabilité** des ressources numériques d'un organisme.

ZRR – *Zone à Régime Restrictif*
Zone soumise à des règles d'accès strictes dans le cadre du PPST, pour protéger des activités scientifiques sensibles.

5. Références réglementaires et techniques

Référentiel	Version	Date	Statut	Lien
Politique de sécurité des systèmes d'information de l'État (PSSIE)	V1.0	17/07/2014	Officielle	https://www.ssi.gouv.fr / https://www.legifrance.gouv.fr
Guide ANSSI d'élaboration de PSSI	–	2004	Toujours en vigueur	https://www.ssi.gouv.fr/guide/guide-pour-lelaboration-dune-pssi
CERT-FR – Bonnes pratiques	–	2025	Actif	https://www.cert.ssi.gouv.fr
RENATER – Documentation sécurité réseau	–	2025	Actif	https://www.renater.fr
CNIL – RGPD et droits numériques	–	2025	Actif	https://www.cnil.fr