PSSI-CNOUS

La Politique de Sécurité des Systèmes d'Information du CNOUS

1 Le mot de la Présidente

Assurer la sécurité de notre numérique est vital pour le fonctionnement du CNOUS et plus généralement du réseau des Crous notamment au regard du service que nous devons garantir aux étudiants.

Les « Cyber menaces » sont en perpétuelle évolution, toujours plus dangereuses notamment avec une nocivité accrue par l'utilisation de l'IA.

Face la multiplication des risques, nous avons l'obligation de protéger au mieux notre patrimoine de données et de garantir la continuité de nos activités au service des Crous et de l'ensemble des étudiants

Au travers de la PSSI, je m'engage et engage le CNOUS à mettre en œuvre **le niveau de sécurité le plus efficient possible pour son numérique**.

La sécurité du numérique est un des axes prioritaires énoncées dans le projet de réseau 2024-2028. Chaque année, dans le budget du CNOUS, des moyens importants sont alloués pour soutenir notre politique de sécurité.

Chaque agent a un rôle et des responsabilités en matière de sécurité de l'information. Conscient que l'humain joue un rôle majeur, j'engage le CNOUS à renforcer la sensibilisation et la formation de tous ses agents à ces enjeux et défis dans le cadre de cette PSSI.

Bénédicte DURAND

Présidente – CNOUS

(Signature)

2 Introduction

2.1 Présentation générale de la politique

Le présent document constitue la Politique de Sécurité des Systèmes d'Information du CNOUS (PSSI-CNOUS).

Cette PSSI s'appuie et respecte les principes définis notamment dans le textes et référentiels suivants :

- La Politique de Sécurité des SI de l'Etat (PSSI-E) : https://www.legifrance.gouv.fr/circulaire/id/38641
- Le Référentiel Général de sécurité (RGS) : https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/
- L'Instruction Générale Interministériel 1337 (IGI-1337) : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000046503128
- La Politique de Gouvernance de Sécurité Numérique de MESR (PGSN-MESR) : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000050080243
- La Circulaire relative à la sécurité des SI des Crous (Circulaire SSI) : https://ionet.CNOUS.fr/wp-content/uploads/2016/07/Circulaire_SSI-et-ses-annexes.pdf
- La Politique de Sécurité des SI cadrant les objectifs de sécurité pour le réseau des Crous (**PSSI-Cadre**) annexée au présent document

La PSSI du CNOUS définit :

- ➔ Les engagements de l'établissement
- ➔ Le référentiel SSI
- ➔ Les rôles et responsabilités des acteurs en matière de Sécurité des Systèmes d'Information.
- ➔ La Gouvernance et l'organisation sécurités définies afin de piloter et d'animer la communauté sécurité au sein du CNOUS ;

La PSSI du CNOUS a vocation à être connue, elle requiert une adhésion et une prise de conscience de chaque agent. Tout agent doit contribuer à la mise en œuvre de cette politique.

Dans le cadre de ses missions de service public, Le CNOUS gèrent (et met à disposition des Crous) des systèmes d'information au profit de l'ensemble des étudiants et des agents du réseau des Crous. Ces systèmes sont de plus en plus exposés.

Le CNOUS a le devoir et l'obligation de protéger son patrimoine numérique afin de garantir le meilleur niveau de service et de sécurité à tous les usagers et utilisateurs (étudiants, agents du réseau des Crous, …).

2.2 Les engagements du CNOUS

Au travers de cette PSSI, **le CNOUS s'engage à** :

- ➔ **Préserver le patrimoine numérique du CNOUS et des CROUS, y compris les savoir-faire et le développement de ces savoir-faire ;**
- ➔ **Respecter et faire respecter les obligations légales, réglementaires et contractuelles tout en anticipant au mieux les changements réglementaires et les exigences gouvernementales ou ministérielles ;**
- ➔ **Assurer la continuité des processus et des activités métiers, tout en garantissant le meilleur niveau de sécurité aux usagers ;**
- ➔ **Renforcer la confiance des utilisateurs et des usagers envers le système d'information qui se doit d'être toujours plus sécurisé et performant ;**
- ➔ **Publier annuellement un rapport de la sécurité du numérique du CNOUS (rapport qui est communiqué au HFDS du ministère chargé de l'enseignement supérieur)**

Une démarche de mise en sécurité du numérique se construit dans une logique d'amélioration continue.

Le CNOUS s'engage à mettre en œuvre une démarche basée sur :

- **Le respect des principes et règles définis dans la PSSI-Cadre (annexée au présent document) ainsi que les référentiels et réglementations en vigueur (*en particulier la Politique de Sécurité des Systèmes d'Information de l'Etat -PSSIE, le règlement général sur la protection des données -RGPD, la Politique de Gouvernance de la Sécurité Numérique -PGSN du ministère chargé de l'enseignement supérieur*) ;**
- **L'application de ces principes et règles par les fournisseurs de services numériques en contrat avec le Cnous ;**
- **La mise en œuvre des principes et plans d'action définis dans la Circulaire relative à la sécurité des systèmes d'information des Crous ;**
- **L'amélioration constante et l'évaluation régulière du niveau de sécurité de ses SI ;**
- **Une démarche proactive notamment au travers d'homologations (RGS) de ses SI les plus sensibles (conformément aux procédures définies par l'ANSSI) ;**
- **La sensibilisation et la formation de tous ses agents sur les risques et enjeux liés à la SSI ;**
- **L'accompagnement des Crous dans la mise en œuvre de leur PSSI.**

2.3 Référentiel de la Sécurité des Systèmes d'Information du Cnous

La Sécurité des Systèmes d'Information au sein du CNOUS et des CROUS ne se limite pas à des aspects techniques. Elle englobe également des dimensions humaines, organisationnelles, fonctionnelles et applicatives.

La démarche de sécurité, adaptée aux besoins et à la maturité du CNOUS et de chaque CROUS en matière de Sécurité des Systèmes d'Information, se décline dans la PSSI-Cadre (en annexe) en plusieurs politiques thématiques (orientées Technique) et Standards pragmatiques (orientés - Opérationnels et Utilisateurs).

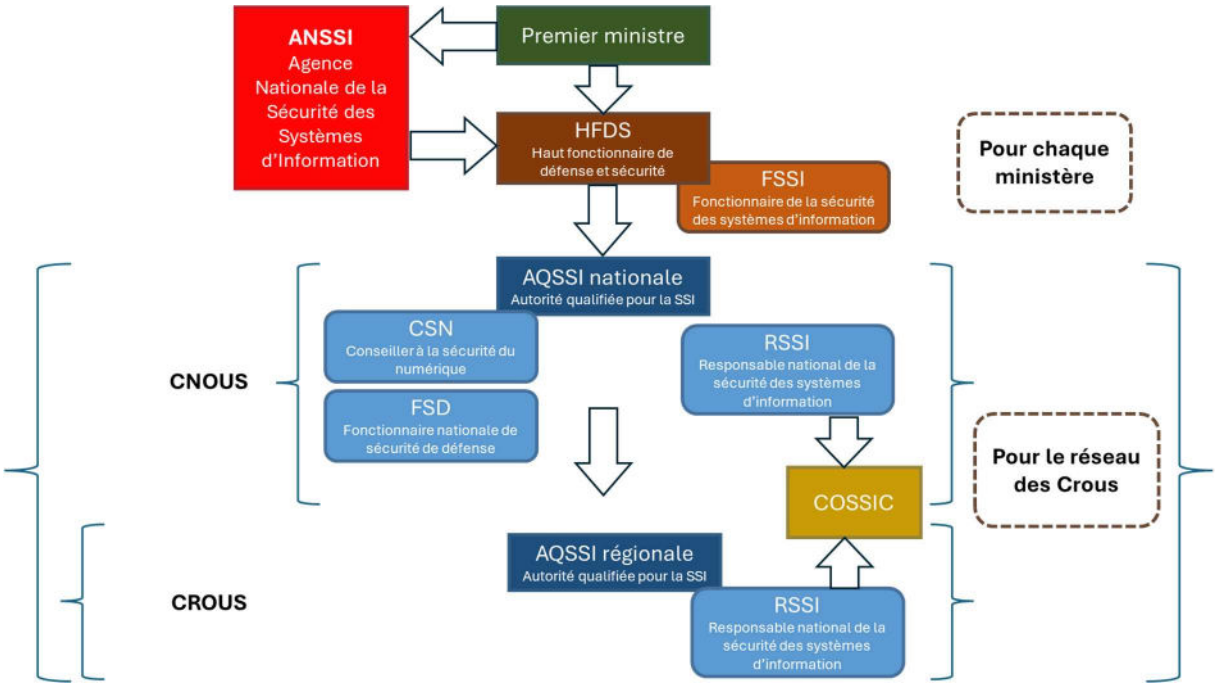
Le tableau ci-dessous offre une vue d'ensemble des axes (définis dans la PSSI-Cadre mise en annexe) que le CNOUS s'engage à couvrir.

Enjeux	Besoin de sécurité	Politiques thématiques / Standards
Sécurité des usagers	- Garantir la protection des données sensibles des étudiants et des personnels - Résilience	- **GRC -** Gouvernance, risques et conformité - **GIA -** Gestion des identités et des accès - **CAI -** Continuité d'activité informatique
Image et confiance	- Maitriser les risques du SI - Gérer les accès aux données - Cloisonner les réseaux - Gérer les actifs informatiques	- **GRC -** Gouvernance, risques et conformité - **SRX -** Sécurité et exploitation des réseaux - **GTE** - Gestion des traces et des évènements de sécurité - **GIA -** Gestion des identités et des accès - **GIS -** Gestion des incidents de sécurité - **ADM -** Administration des ressources informatiques - **GBI -** Gestion des biens - **MCS -** Maintien en conditions de sécurité - **GIS -** Gestion des incidents de sécurité - **CAI -** Continuité d'activité informatique - **SPT -** Sécurité du poste de travail - **SAM -** Sécurité applicable à la mobilité - **OPI -** Organisation des projets informatiques - **SDP -** Sécurité des données personnelles - **SDEV -** Sécurité des développements
Légal et réglementaire	- Gérer la conformité avec les réglementations	- **GRC -** Gouvernance, risques et conformité - **GTE** - Gestion des traces et des évènements de sécurité - **GIS -** Gestion des incidents de sécurité - **SFP -** Sécurité des fournisseurs et partenaires - **SDP -** Sécurité des données personnelles
Economiques et financiers	- Lutter contre la fraude - Gérer les contrôles et la conformité - Protéger les relations avec les tiers	- **GRC -** Gouvernance, risques et conformité - **GIA -** Gestion des identités et des accès - **GIS -** Gestion des incidents de sécurité - **SFP -** Sécurité des fournisseurs et partenaires

3 Rôles et responsabilités

L'atteinte des enjeux définis par la PSSI nécessite une organisation structurée et dirigée, définissant clairement les rôles et responsabilités de l'ensemble des intervenants, ainsi que les moyens mis à leur disposition.

Au regard des dispositions du décret n° 2022-513 du 8 avril 2022 complété par l'arrêté du 26 octobre 2022 ainsi que du PGSN ministériel et tel que cela a été défini dans la circulaire SSI du réseau , la chaîne fonctionnelle au niveau interministériel, ministériel et de l'établissement est constituée ainsi :



En complément de cette chaîne fonctionnelle, tout service et tout agent ont leur rôle à jouer pour garantir le meilleur niveau de sécurité du numérique du CNOUS.

3.1 Autorité Qualifiée de la Sécurité des Systèmes d'Information (AQSSI)

La présidente ou le président du CNOUS porte le rôle d'AQSSI (Autorité Qualifiée pour la SSI) pour le CNOUS et AQSSI nationale pour le réseau des CROUS.

L'AQSSI est responsable de la sécurité des systèmes d'information de l'établissement. Elle ne peut déléguer cette responsabilité.

L'AQSSI alloue les ressources nécessaires pour mener à bien les projets de transformation numérique de son périmètre de responsabilité et s'assure à ce titre que les risques numériques sont gérés. Ces éléments sont tenus à la disposition du fonctionnaire de sécurité des systèmes d'information.

L'AQSSI s'assure de la bonne prise en compte de ses orientations en matière de sécurité numérique pour le Cnous et les Crous.

Sur son périmètre de responsabilité, l'AQSSI contrôle l'application des exigences de sécurité numérique auxquelles elle est soumise. Elle intègre dans la programmation de ses contrôles internes le volet relatif à la sécurité numérique. Elle accepte notamment les risques résiduels identifiés.

Elle remet annuellement un rapport dans lequel elle intègre l'évaluation du niveau de sécurité numérique et une synthèse des incidents de sécurité ayant impacté ses missions.

L'AQSSI s'assure de l'élaboration, de la mise en œuvre et du maintien, notamment au travers d'exercices, des plans de continuité et de reprise des activités relevant de son domaine de responsabilité face à des incidents de sécurité.

L'AQSSI s'assure de la définition et de la mise en œuvre d'un processus de gestion des incidents de sécurité ainsi que d'une organisation de gestion de crise face aux incidents de sécurité, en lien avec la chaine ministérielle et sectorielle de traitement des incidents de sécurité des SI.

Pour l'assister dans l'exercice de ses prérogatives, l'AQSSI nomme un **Conseiller à la Sécurité Numérique.**

3.2 Conseiller à la sécurité du Numérique (CSN)

Le CSN intervient en tant que conseiller stratégique en matière de cyber sécurité auprès de l'AQSSI et doit :

- Veiller à la cohérence globale de la sécurité du SI ;
- Conseiller la gouvernance sur les orientations à prendre en matière de maîtrise des risques numériques ;
- Reporter à l'AQSSI les activités liées à la sécurité des systèmes d'information ;
- Coordonner (et contribuer à) l'élaboration de la PSSI et le contrôle de son application ;
- Dresser une cartographie des missions critiques et des risques stratégiques, puis identifie les SI qui les soutiennent,
- Accompagner et conseiller l'AQSSI en matière d'homologation ;
- Conseiller l'AQSSI dans sa prise de décision en cas de crise cyber ;
- Coordonner la mise en œuvre des orientations de l'AQSSI en matière de sécurité numérique ;
- S'assurer de la bonne prise en compte des besoins de sécurité du métier par les fournisseurs de services numériques ainsi que de la mise en œuvre des démarches de maîtrise des risques numériques ;
- Conseiller l'AQSSI en vue des instances stratégiques ministérielles de la sécurité numérique et la représenter lors des instances ministérielles de pilotage de la sécurité numérique ;
- Contribuer à l'élaboration du rapport annuel de sécurité que l'AQSSI remet au haut fonctionnaire de défense et de sécurité (HFDS) ;
- Promouvoir des actions de sensibilisation au risque numérique et de diffusion des bonnes pratiques au sein de son périmètre.

3.3 Fonctionnaire de Sécurité de Défense (FSD)

Le FSD est le relai fonctionnel du Haut Fonctionnaire de Défense et sécurité ministériel pour le réseau des Crous. Le FSD est placé auprès du président ou présidente du CNOUS qu'il assiste sur l'ensemble du périmètre défense et sécurité.

Il a pour missions d'intervenir sur plusieurs domaines de la sécurité publique et de la défense :

- La Protection du Potentiel Scientifique et Technique (PPST) et Zone à régime restrictif (ZRR) ;
- La mise en œuvre des plans de défense (Vigipirate, pandémie, PPMS, …) ;
- La gestion de crise et continuité d'activité ;
- La protection du secret de la Défense Nationale.

3.4 Responsable de Sécurité des Systèmes d'Information (RSSI)

Le RSSI est le chef d'orchestre de la démarche sécurité du système d'information. Il est directement rattaché à l'AQSSI et au CSN.

Le RSSI du CNOUS est également RSSI national du réseau des Crous. Dans ce rôle, il anime le réseau des RSSI de CROUS.

Le RSSI a pour missions de :

- Contribuer activement à l'élaboration d'une politique de sécurité (et de sa mise à jour) cohérente admise par tous et la mettre en œuvre ;
- S'assurer de la bonne application de la PSSI ;
- Coordonner l'analyse de risque du SI ;
- Suivre et faire appliquer les différents plans d'actions pour traiter les risques et ainsi pouvoir les faire accepter par la direction ;
- Sensibiliser l'ensemble des personnels du CNOUS sur la thématique de la Sécurité des systèmes d'information ;
- Communiquer à tous les niveaux des informations relatives à la sécurité des systèmes d'information ;
- Animer les différents comités liés à la sécurité des systèmes d'informations ;
- Gérer les incidents de sécurité et faire le lien avec les autorités compétentes ;
- Intégrer la sécurité dans les projets et dans les relations avec les tiers ;
- Participer aux échanges et comités au niveau national avec les CROUS.

3.5 La Sous-direction du numérique (SDN)

La SDN gère l'ensemble du périmètre du numérique pour l'établissement et à ce titre, les responsabilités suivantes lui incombent :

- Garantir la déclinaison technique et opérationnelle des exigences de la PSSI ;
- Reporter au RSSI toutes difficultés rencontrées dans l'implémentation de solutions pour satisfaire les exigences de la PSSI ;
- Assister les équipes d'exploitation pour l'intégration de sécurité dans les projets du SI ;
- Reporter au RSSI tout incident de sécurité détecté par l'équipe SI ou les utilisateurs.

3.6 Sous-directions et services Métiers

Les sous-directions métiers sont également parties prenantes de la démarche sécurité des systèmes d'information au sein de leur service.

A leur niveau, différentes responsabilités leurs incombent :

- Promouvoir la sécurité au sein de leurs directions et services ;
- S'assurer de l'implémentation des mesures définies dans la PSSI au sein de leurs directions et services ;
- Participer à l'évaluation des risques et à l'identification des risques résiduels sur leur périmètre ;
- Faire respecter les dispositifs relatifs à la sécurité du numérique par les agents sous leur responsabilité ;
- S'assurer d'avoir une continuité d'activité fonctionnelle au sein de leurs directions et services en cas de sinistre.

3.7 Le Comité Opérationnel de la Sécurité des Systèmes d'Information des Crous (COSSIC)

Créé par la circulaire SSI référencée ci-dessus, le COSSIC a pour rôles sur l'ensemble du périmètre du réseau des Crous, de :

- Conseiller les RSSI du réseau des Crous sur l'ensemble du domaine de la SSI ;
- Soutenir les actions dans le cadre du traitement d'incident de sécurité
- Proposer des actions préventives ou curatives sous forme d'avis ou de motion

Le CNOUS s'engage à impliquer le COSSIC à chaque fois que nécessaire et à l'associer dans la prise de décisions importantes relatives à la cyber sécurité.

3.8 Utilisateurs (agents)

Les utilisateurs, conformément à ce qui est écrit dans la charte relative au numérique, sont responsables de l'usage qu'ils font des ressources informatiques et de toutes informations qu'ils créent, manipulent, partagent ou diffusent. Ils doivent être conscients des règles de sécurité, des bonnes pratiques et de leurs responsabilités en la matière. Ils ont le devoir de remonter tout incident ou faille de sécurité dont ils sont témoins de manière directe ou indirecte.

4 Gestion de la sécurité des systèmes d'information

4.1 Gouvernance

La gouvernance de la sécurité des systèmes d'information est essentielle pour assurer une gestion cohérente et efficace de la sécurité au sein du CNOUS.

La gouvernance de la sécurité des systèmes d'information est pilotée au travers d'un comité dédié.

Ce comité a pour objectifs de :

- Aligner et suivre la feuille de route vis-à-vis de la stratégie SSI
- Maitriser les niveaux de risques de son numérique via des indicateurs et tableaux de bord
- Coordonner et suivre les actions et de s'assurer d'avoir les ressources nécessaires pour y parvenir
- Arbitrer des choix ou des sujets relatifs à la sécurité du système d'informations (exemple : choix d'une solution, dérogation à une exigence de la PSSI, etc.)

Les membres de ce comité sont : la Direction du CNOUS, le CSN, le FSD, le RSSI, le DPO, le Sous-directeur du numérique et le président du COSSIC. Peuvent associer à ce comité d'autres acteurs de l'institution en fonction de l'actualité et thèmes abordés (Sous-directions métiers).

Ce comité se réunit à minima un fois par semestre et autant que nécessaire en cas de cybercrise.

Sur proposition du RSSI, ce comité valide le **rapport annuel de la sécurité du numérique** du CNOUS.

4.2 Gestion de la sécurité par le risque

Les activités liées à la sécurité des systèmes d'information du CNOUS doivent être pilotées par les risques. Le CNOUS met en œuvre une démarche d'analyse de risques basée sur une méthode connue (exemple : EBIOS Risk Manager de l'Agence Nationale de Sécurité des Systèmes d'Information) permettant de dresser une cartographie des risques encourus, d'identifier les actions requises pour les réduire à un niveau acceptable et de suivre leurs évolutions dans le temps.

La réalisation d'une analyse de risques de sécurité des systèmes d'information fixe un cap, permet de définir un niveau de sécurité adapté aux besoins et contraintes du CNOUS.

4.3 Besoins de sécurité

La politique de sécurité du numérique a pour objectif de couvrir au mieux les 3 axes :

- *Disponibilité :* propriété d'être accessible et utilisable à la demande par une entité autorisée
- *Intégrité :* propriété d'exactitude et de complétude
- *Confidentialité :* propriété selon laquelle l'information n'est pas diffusée ni divulguée à des personnes, des entités ou des processus non autorisés.

Les définitions de ces axes sont issues de la norme ISO/IEC 27000 relatives au Système de management de la sécurité de l'information.

4.4 La Revue stratégique annuelle de la sécurité des SI

La revue annuelle de la stratégie de sécurité des systèmes d'information est une étape cruciale pour assurer que les politiques, procédures et mesures de sécurité restent pertinentes, efficaces et alignées avec les objectifs de l'organisation.

La Revue Stratégique de la Sécurité du Système d'Information a pour objectif de :

- Valider la Politique de Sécurité du Système d'Information et ses évolutions ;
- S'assurer de la cohérence entre la stratégie sécurité SI et les stratégies d'évolution du CNOUS ;
- Valider les plans d'action et les budgets en matière de Sécurité du Système d'Information ;
- Effectuer le suivi et l'arbitrage des projets stratégiques de sécurité des SI ;
- Arbitrer et valider les risques liés au système d'information.

Cette revue stratégique est retranscrite dans **le rapport annuel de la sécurité du numérique** du CNOUS.

5 Annexe

5.1 La PSSI Cadre

Document annexé à diffusion restreinte : Pssi-Cadre-Cnous-Crous.pdf

ou Intranet SSI :

https://ssi.in.nuonet.fr/wiki/doku.php?id=documents_ssi:pssi:pssi-public