Présidence
Vice-Président du conseil d'administration
Franck LE DERF

Direction Générale des services
Pascale LAINE-MONTELS

Affaire suivie par :
Victorine MENDY
Responsable des Instances
02.35.14.67.69
secretariatca@univ-rouen.fr

Conseil d'administration - URN
18 octobre 2024
Délibération n°CA-2024-13

À l'ouverture de la réunion, le quorum est atteint par 26 votants, dont 10 membres représentés

Validation de la politique de sécurité du système d'information (PSSI)

- Vu le décret n° 2022-513
- Vu l'arrêté du 26 octobre 2022
- Vu l'article L712-3 du code de l'éducation
- Vu le dossier en annexe

Approbation de la politique de sécurité du système d'information

Pour	26
Contre	0
Abstention	0

Le conseil d'administration approuve la politique de sécurité du système d'information

Fait à Rouen, le 18 octobre 2024

Le président de l'Université de Rouen Normandie

Laurent YON

Présidence
Direction Générale des Services

Mont-Saint-Aignan, le 07 octobre 2024

Note
À l'attention de mesdames et messieurs les membres du conseil d'administration
Séance du 18 octobre

Objet : Présentation de la Politique de Sécurité du Système d'Information (PSSI)

1. Objectifs principaux

La Politique de Sécurité du Système d'Information (PSSI) de l'URN définit les principes directeurs et les orientations visant à assurer la sécurité de nos systèmes d'information. Elle s'inscrit dans une démarche globale de protection des ressources numériques, en cohérence avec les enjeux de continuité d'activité, de confidentialité, d'intégrité et de disponibilité des informations.

La perte, altération ou la divulgation de données relatives aux contrats, à la gestion, à la communication, à la recherche, à l'enseignement en général, ou encore aux données à caractère personnel peuvent avoir un impact critique sur le fonctionnement, la pérennité financière et l'image de l'URN.

Le secteur public (dont les universités) n'est pas épargné par les attaques informatiques (rançongiciel, hameçonnage, vol de données, défiguration de site internet, etc.) qui sont de plus en plus sophistiquées et exponentielles. Dans un monde toujours plus interconnecté et exposé en permanence aux cybermenaces, la Sécurité du Système d'Information est essentielle à l'université de Rouen Normandie pour maintenir son activité et son développement. La pérennité ne pourra être durable que par une capacité à se remettre continuellement en question afin d'anticiper les menaces pouvant porter atteinte au patrimoine informationnel et numérique.

La mise en œuvre de cette PSSI permettra non seulement de protéger nos systèmes et données, mais aussi de renforcer la confiance de nos partenaires et utilisateurs tout en assurant la pérennité de nos activités.

Le respect de cette politique est une responsabilité partagée par l'ensemble des étudiants et personnels.

Face à ces enjeux, des objectifs se dégagent pour répondre aux besoins de confidentialité (C), d'intégrité (I), de disponibilité (D) et de traçabilité des données (T). L'Université de Rouen Normandie doit également répondre à des exigences légales et réglementaires.

Les objectifs stratégiques de la PSSI sont les suivants :

- Maintenir en condition de sécurité le système d'information 7j/7 et 24h/24 ;
- Assurer la confidentialité, l'intégrité et la disponibilité des données (administratives, contractuelles, personnelles, formations, recherche, etc.) ;
- Promouvoir une culture partagée de la sécurité de l'information ;
- Veiller au respect des exigences définies par les contraintes légales et réglementaires ;
- Connaitre et maitriser les risques cyber ;
- Assurer la résilience du système d'information en cas d'incident de sécurité ;
- Définir un niveau de sécurité lors de l'intégration de nouvelles interconnexions au SI ;
- Veiller au respect des exigences définies par les contraintes règlementaires et fiscales ;
- Garantir l'image de marque de l'université.

Ces objectifs stratégiques se déclinent en directives opérationnelles qui seront décrites de manière thématique dans la PSSI Opérationnelle. Cette dernière s'appuie sur des normes et référentiels relatifs à la sécurité de l'information (ex : la PSSI-E, ISO 27001,27002, etc. guides ANSSI, RGPD, Nis2, etc.)

Il est demandé aux administrateurs de se prononcer sur la politique de sécurité du système d'information de l'université.

Politique de Sécurité du Système d'Information

Version 0.1

Diffusion limitée

Sommaire

1. Objet

Ce document constitue la Politique de Sécurité du Système d'Information de l'Université Rouen Normandie, notée **PSSI** dans la suite du document.

La PSSI, **approuvée par le conseil d'administration de l'établissement**, définit notamment les enjeux et objectifs stratégiques pour la sécurisation du Système d'Information (SI). Ce même document précise également les engagements en matière de pilotage de la Sécurité du Système d'Information (SSI), permettant d'assurer la pérennité de la démarche dans le temps.

Il sera complété par une **PSSI Opérationnelle** regroupant les directives thématiques sur les domaines clés liées à la sécurité physique et logique du Système d'Information.

2. Critères de diffusion

La PSSI doit être connue de l'ensemble des acteurs internes ainsi que le cas échéant, de l'ensemble des personnes (ex : partenaires, prestataires, stagiaires, etc.) accédant au système d'information de l'Université de Rouen Normandie (URN). Néanmoins, la diffusion des éléments constituant le corpus documentaire de la PSSI est restreinte car celui-ci peut contenir des informations sensibles. **Chaque document mentionne une liste de diffusion définissant les personnes ou catégories de personnes autorisées à accéder au contenu**.

Lorsque nécessaire et par souci de confidentialité, un extrait des informations pertinentes sollicité par un tiers pourra être communiqué par le RSSI au cas par cas et sur demande écrite et justifiée.

3. Périmètre

La PSSI est un document applicable à la totalité du système d'information de l'URN incluant toutes les informations matérielles ou logicielles nécessaires à leur gestion (création, acquisition, traitement, stockage, diffusion, destruction, etc.) où qu'elles se trouvent (campus).

Cas des unités multi-tutelles ou hébergées :

Le système d'information des unités de recherche multi-tutelles est également concerné par la PSSI de l'Université, sauf si une autre disposition a été exprimée dans le cadre des contrats de partenariat passés entre l'Université et une ou plusieurs autre(s) tutelle(s) de l'unité. Si plusieurs PSSI sont applicables, la PSSI la plus exigeante s'appliquera.

Définitions :

- **Collaborateur** : toute personne impliquée dans le SI (titulaires, contractuels, enseignants/chercheurs, sous-traitant, étudiants/stagiaire, supports, etc.).
- **Information** : toute donnée stockée au sein de l'URN, au format papier ou numérique.
- **Matériel** : tout élément physique supportant les processus (ordinateur portable, serveur, mobiles, imprimante, support amovible, onduleur, armoire de stockage, etc.).
- **Logiciel** : tout programme ou exécutable contribuant aux opérations sur les données (système d'exploitation, logiciel de supervision, suite bureautique, etc.).
- **Réseau** : toute forme d'interconnexion des composants matériels et logiciels du SI (ligne spécialisée, réseau téléphonique, réseau IP, etc.).
- **Site** : tout emplacement géographique appartenant à l'URN ou mis à disposition (bureaux, laboratoires, amphithéâtres, salles de cours, etc.).

4. Enjeux et objectifs stratégiques

4.1. Enjeux

Le Système d'Information de l'URN est constitué par les processus métiers et par les outils déployés, il est indispensable pour les activités d'enseignement, de recherche et de gestion. L'université dispose d'un patrimoine informationnel crucial sur lequel reposent sa pérennité, sa légitimité et sa capacité à maintenir et développer ses services et missions. Dépendante du bon fonctionnement du SI, **la sécurité est donc un enjeu majeur dans la conception et le maintien du Système d'Information de l'Université de Rouen Normandie.**

La perte, l'altération ou la divulgation de données relatives aux contrats, à la gestion, à la communication, à la recherche, à l'enseignement en général, ou encore aux données à caractère personnel auraient un impact critique sur le fonctionnement, la pérennité financière et l'image de l'URN.

Le secteur public n'est pas épargné par les attaques informatiques (rançongiciel, hameçonnage, vol de données, défigurations de sites internet, etc.) qui sont de plus en plus sophistiquées et exponentielles. Dans un monde toujours plus interconnecté et exposé en permanence aux cybermenaces, **la Sécurité du SI est essentielle à l'université de Rouen Normandie pour maintenir son activité et son développement**. Le maintien du SI ne pourra être assuré que par une capacité à se remettre continuellement en question afin d'anticiper les menaces pouvant porter atteinte au patrimoine informationnel et numérique.

4.2. Objectifs stratégiques

Face à ces enjeux, des objectifs se dégagent pour répondre aux **besoins de confidentialité (C), d'intégrité (I), de disponibilité (D) et de traçabilité des données (T).** L'URN doit également répondre à des exigences légales et réglementaires.

Les objectifs stratégiques sont les suivants :

- Maintenir en **condition de sécurité** le système d'information 7j/7 et 24h/24 ;
- Assurer la **confidentialité, l'intégrité et la disponibilité** des données (administratives, contractuelles, personnelles, formations, recherche, etc.) ;
- Promouvoir une **culture partagée** de la sécurité de l'information ;
- Veiller au **respect des exigences** définies par les contraintes légales et réglementaires ;
- Connaitre et maitriser les **risques cyber** ;
- Assurer la **résilience du système d'information** en cas d'incident de sécurité ;
- Définir un niveau de sécurité lors de **l'intégration de nouvelles interconnexions** au SI ;
- Veiller au respect des exigences définies par les **contraintes règlementaires et fiscales** ;
- Garantir **l'image** de marque de l'université.

Ces objectifs stratégiques se déclinent en directives opérationnelles décrites de manière thématique dans la **PSSI Opérationnelle**. Cette dernière s'appuie sur des référentiels et normes relatifs à la sécurité de l'information (ex : norme ISO 27001[1], NIS 2[2], ANSSI[3], etc.).

5. Gouvernance et organisation de la SSI

La chaîne organisationnelle de la SSI repose sur plusieurs acteurs et niveaux hiérarchiques, chacun ayant des responsabilités spécifiques pour assurer la sécurité et la résilience des systèmes d'information.

Les acteurs de la gouvernance en matière de SSI au sein de l'URN sont :

- Le Président ;
- Le Fonctionnaire Sécurité Défense (FSD) ;
- L'adjoint au FSD ;
- Le Comité de Pilotage du Numérique (COPNUM) ;
- Le Responsable de la sécurité des systèmes d'information (RSSI) ;
- le Délégué à la Protection des Données (DPD) ;
- Les correspondants Sécurité des systèmes d'information (CSSI) ;
- La Direction des systèmes d'information (DSI).

5.1. Autorité Qualifiée de la sécurité des Systèmes d'information

Au sein de l'Université, la responsabilité formelle de la SSI relève de son président en sa qualité d'Autorité Qualifiée pour la Sécurité des Systèmes d'Information (AQSSI). Il peut être juridiquement responsable en cas d'incident de sécurité.

5.2. Le Fonctionnaire Sécurité Défense

Le FSD est le représentant de l'État dans l'établissement en matière de sécurité et de défense. Il assure un rôle de coordination, de conseil, d'information et de mise en œuvre dans le cadre de la protection du potentiel scientifique et technique (PPST), de la protection du secret et de la préparation / exécution des plans de défense et de sécurité.

5.3. L'Adjoint au Fonctionnaire Sécurité Défense

L'adjoint au FSD est sous la responsabilité directe du président d'université et de la Directrice Générale des Services. Il intervient sur plusieurs domaines de la sécurité publique et de la défense comme la PPST, la mise en œuvre locale du plan Vigipirate, la procédure de gestion de crise et la protection du secret de la défense nationale.

Ses actions ont pour but de préserver l'université de toutes atteintes au personnel, au patrimoine matériel et immatériel afin que les missions de l'université s'accomplissent sereinement.

[1] https://fr.wikipedia.org/wiki/ISO/CEI_27001
[2] https://cyber.gouv.fr/la-directive-nis-2
[3] https://cyber.gouv.fr/securiser-son-organisation

5.4. Comité de Pilotage du Numérique

Voir l'article 17-9 des statuts de l'URN définissant les attributions et la composition du comité.

5.5. Le Responsable Sécurité des Systèmes d'Information

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

Le RSSI a pour mission[4] :

- D'identifier les enjeux et les risques de sécurité majeurs pour l'établissement, les formaliser ;
- De décliner les axes et les objectifs stratégiques en matière de cybersécurité et établir un plan d'actions pluriannuel recouvrant également les actions de sensibilisation et la promotion des « bonnes pratiques » ;
- De proposer à la gouvernance un plan d'actions préventives, correctives et prospectives en matière de SSI en collaboration avec les parties prenantes (composantes, laboratoires, directions, services et équipes informatiques) ;
- De coordonner les différents intervenants en cas de problème (présidence, composantes, CERT, RENATER, autorités compétentes, sites extérieurs concernés, etc.) ;
- D'exploiter et relayer les informations relatives à la sécurité reçues via le CERT RENATER, CERTA, le FSSI/HFDS et/ou les correspondants sécurité de l'enseignement supérieur ;
- De définir une politique d'investissement au regard des objectifs de sécurité ;
- D'analyser les besoins de sécurité des nouveaux projets, exprimés en termes de disponibilité, de confidentialité et d'intégrité des données, traçabilité ;
- D'assurer la mise en conformité de l'établissement aux mesures et textes SSI réglementaires applicables ;
- De prévoir en liaison avec le DPD, la sensibilisation des usagers aux aspects de sécurité des données à caractère personnel ;
- D'assurer la veille technologique et prospective pour garantir la sécurité logique et physique du SI ;
- De formaliser la stratégie de cyber-résilience tant pour la continuité (PCA) que pour la reprise d'activités (PRA) ;
- De tenir à jour un registre des incidents de sécurité liés au SI ;
- D'organiser et formaliser un dispositif de gestion de crise sécurité ;
- D'établir annuellement un rapport formalisé du niveau de couverture courant des risques de sécurité SI ;
- D'assurer un rôle de conseil auprès de la gouvernance.

5.6. Correspondants Sécurité des Systèmes d'Information

Les CSSI sont nommés dans les différentes entités de l'URN. Leur fonction est de veiller à l'application de la PSSI de l'URN, dans leur structure respective, et de remonter les éventuels incidents de sécurité.

Chaque responsable d'entité doit désigner un CSSI. Dans le cas de structures de taille importante, il est souhaitable que soient désignés deux CSSI (un titulaire et un suppléant). Dans le cas de petites

[4] Lettre de mission du RSSI en annexe

entités partageant les mêmes infrastructures, la fonction de CSSI peut être mutualisée. La désignation d'un CSSI dans les entités classées (par exemple : zones à régime restrictif (ZRR)) est prioritaire. Le CSSI agit sous l'autorité fonctionnelle du RSSI dans le périmètre de la sécurité.

Il a en particulier pour missions :

- De promouvoir la mise en place d'une PSSI d'unité conforme à la PSSI d'établissement ;
- D'assurer la diffusion de l'information correspondante et notamment les instructions et recommandations ;
- De sensibiliser les utilisateurs aux bonnes pratiques en matière de sécurité des SI ;
- De veiller à la mise en place et l'application des règles de sécurité nécessaires dans leur unité ;
- De veiller à la bonne exploitation des avis des CERT-Renater, CERT-FR, etc. ;
- D'appliquer les mesures demandées par le RSSI de l'URN ;
- De prendre les mesures nécessaires en cas d'incident (ou s'assurer qu'elles sont prises) en liaison si nécessaire avec le RSSI et en veillant à la bonne remontée de l'information ;
- D'établir les rapports d'incidents demandés par le RSSI ;
- De veiller au respect des formalités requises par le règlement général sur la protection des données (RGPD) pour les traitements informatiques de données à caractère personnel ;
- De contribuer à la veille en matière de SSI en lien avec le RSSI.

5.7. La Direction des Systèmes d'Information

La Direction des Systèmes d'Information (DSI) met en œuvre la PSSI et fait appliquer les règles de sécurité au sein du SI. Elle maintient et garantit la disponibilité et le bon fonctionnement des moyens et ressources informatiques.

La DSI participe activement à la veille sécuritaire et technologique en lien avec la RSSI.

Elle vérifie régulièrement la vulnérabilité des infrastructures techniques en collaboration avec le RSSI et l'informe systématiquement des travaux susceptibles d'impacter les dispositifs de sécurité en place ou d'influencer la cartographie des risques.

5.8. Le Délégué à la protection des données

Conformément au RGPD, il est nommé par le Président et a vocation à travailler en lien avec le RSSI.

Le DPD a pour mission :

- D'informer et conseiller le responsable de traitement ainsi que les personnels aux enjeux de la protection des données ;
- De contrôler le respect du règlement et du droit national en matière de protection des données ;
- De conseiller l'université sur la réalisation d'une analyse d'impact relative à la protection des données et en vérifier l'exécution ;
- De coopérer avec l'autorité de contrôle ;
- D'établir, maintenir et communiquer aux personnes en faisant la demande, la liste des traitements réalisés au sein de l'établissement ;
- De procéder aux formalités préalables concernant les traitements soumis à autorisation ou avis de la CNIL ;

- D'accompagner la mise en œuvre des traitements de données à caractère personnel ;
- De recevoir les demandes et les réclamations adressées par les personnes concernées par les traitements, et selon leur nature les instruire ou les transmettre aux services compétents ;
- D'alerter le responsable des traitements sur l'existence de manquements au RGPD ;
- De rédiger et remettre au responsable des traitements un bilan annuel des actions menées au titre de ses fonctions de DPD ;
- De participer au réseau métier regroupant les DPD de l'enseignement supérieur et de la recherche.

6. Obligations légales et réglementaires

Cette politique répond au cadre législatif national de se conformer à la Politique de Sécurité des Systèmes d'Information de l'État (PSSIE) et aux instructions de la directive interministérielle n°901[5] relative à la protection des Systèmes d'Information traitant des "informations sensibles non classifiées de défense".

En cas d'absence de règles et mesures de sécurité spécifiques, l'URN 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[6], est un ensemble de règles de protection applicables aux SI de l'État.

7. Gestion des exceptions à la PSSI

Tous les écarts par rapport aux règles de sécurité fixées sont considérés comme des failles de sécurité et ne devraient pas être autorisés. Néanmoins, **certaines règles établies peuvent faire l'objet d'exception**. Dans ce cas, les demandes devront être formalisées auprès du RSSI qui donnera un avis. Ces avis seront proposés pour validation finale par le Président**.**

Chaque exception sera tracée et revue annuellement (au minimum) afin de confirmer sa légitimité.

8. Gestion des non conformités

La conformité à la PSSI de l'URN est vérifiée par des contrôles réguliers (surveillance dans le cadre de l'exploitation, revue des droits d'accès, analyse des logs système et réseau, analyse des incidents de sécurité, remontées des utilisateurs, etc.).

Le RSSI s'assure de la mise en œuvre effective des règles de sécurité prévues par la PSSI. Il établit un bilan annuel de l'état d'avancement de sa mise en œuvre, présenté devant le CA.

[5] https://cyber.gouv.fr/protection-de-linformation-sensible-et-diffusion-restreinte
[6] https://www.legifrance.gouv.fr/circulaire/id/38641

9. Engagement de l'établissement

9.1. Lettre d'engagement

L'URN est consciente que le maintien de son activité ne pourra être réalisé que par la capacité à se remettre continuellement en question afin d'anticiper les menaces informatiques pouvant porter atteinte aux activités et aux données des personnels et de l'entité en général. Dans la continuité de la démarche de sécurité de l'URN, la PSSI est intégrée à la stratégie générale de l'établissement. Elle a pour but de répondre aux objectifs de sécurité suivants :

- Maintenir en condition de sécurité l'infrastructure ainsi que le SI en mettant à disposition des moyens adaptés ;
- Maintenir en condition opérationnelle le SI afin de garantir une reprise d'activité rapide en cas d'incident majeur ;
- Veiller à la confidentialité et à l'intégrité des données manipulées ;
- Assurer la sécurité sur toute la chaîne de traitement de l'information en considérant l'ensemble de l'écosystème (utilisateurs, administrateurs, prestataires, etc.) ;
- Promouvoir une culture partagée de la sécurité de l'information ;
- Veiller au respect des exigences réglementaires et légales (PSSI-E, NIS 2, RGS, RGPD, etc.) ;
- Inscrire l'Université dans les bonnes pratiques préconisées par les référentiels et guides ANSSI, les normes ISO 27001,27002, 27005, etc.

Ces objectifs stratégiques ne pourront être atteints que par l'engagement de chacun à appliquer, contribuer et promouvoir les directives de sécurité dans leurs activités quotidiennes.

Dans ce contexte, l'établissement veille à ce que la SSI, soit un axe stratégique de sa politique. La Présidence et la direction générale des services s'assurent que les dispositifs mis en place soient efficaces et s'inscrivent dans une démarche d'amélioration continue.

10. ANNEXES

Fondements de la Politique de Sécurité du Système d'Information

L'établissement au travers de sa présidence et de sa direction générale des services soutiennent la politique de sécurité, au travers d'actions en mettant en œuvre des actions concrètes à différents niveaux visant notamment à sensibiliser les usagers. La PSSI est donc suivie d'une PSSI opérationnelle et des procédures idoines.

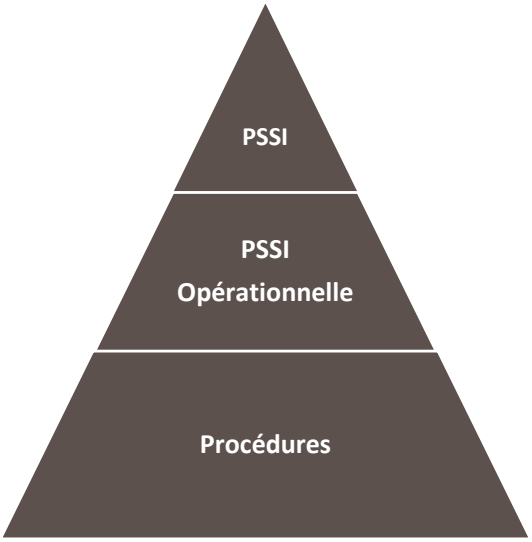
Structure de la documentation

La PSSI est organisée en 3 niveaux :

Le 1er niveau correspond au présent document. C'est le document de référence qui fixe les enjeux, les principes de gouvernance et les principes fondamentaux de sécurité.

Le 2e niveau correspond aux directives de sécurité définis au sein de la politique opérationnelle. Il s'agit des règles de sécurité définies en fonction notamment des guides de bonnes pratiques de sécurité (ISO 27001,27002, Guide d'hygiène de l'ANSSI, NIS2, RGPD, RGS, etc.). Ces directives sont élaborées pour régir et traiter une thématique de sécurité (gestion des habilitations, sécurité physique, etc.).

Le 3e niveau correspond aux procédures qui accompagnent la PSSI opérationnelle



Mise en application

Les objectifs de sécurité de l'information qui ont été définis précédemment font l'objet d'une **déclinaison en actions et recommandations** au sein du document **PSSI Opérationnelle**. Ces directives doivent être mises en application par l'ensemble des acteurs du SI pour être en conformité avec la présente politique.

De manière générale, **chaque évolution du SI** intègre la sécurité en prenant en compte les exigences de la PSSI Opérationnelle en fonction de leurs **besoins de sécurité** exprimés en termes de confidentialité, d'intégrité, de disponibilité et de traçabilité des données et des traitements.

Révision

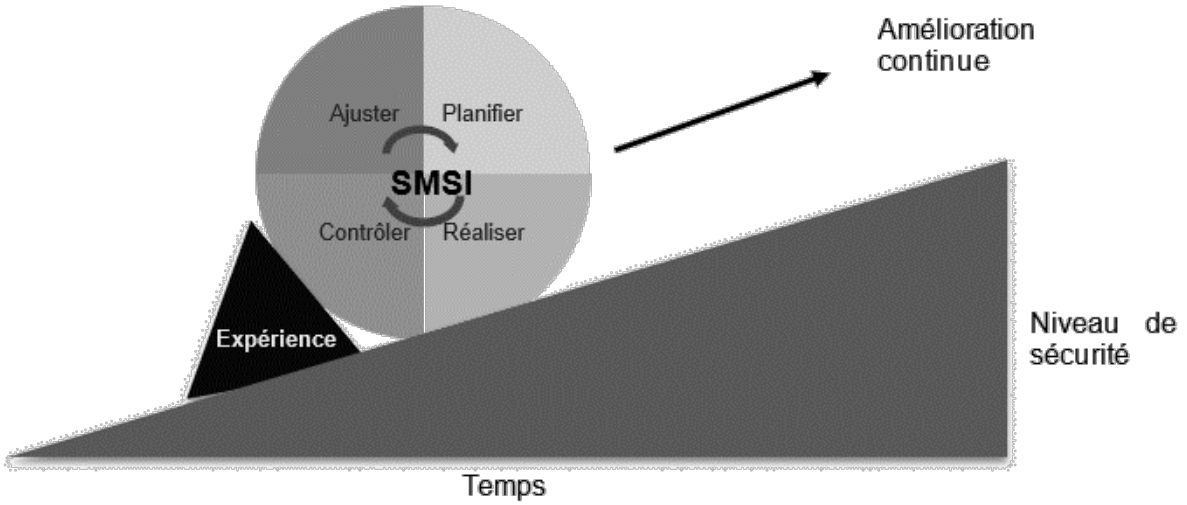
La PSSI est revue, a minima, **annuellement** pour vérifier son efficacité et son adéquation avec les **objectifs stratégiques.** La révision est réalisée à intervalle régulier ou lors de l'identification de toute opportunité d'amélioration telle que :

- Le retour d'expérience suite à la mise en œuvre de règles de sécurité ;
- Le contrôle des règles de sécurité ;
- L'évolution des bonnes pratiques ou de l'état de la menace ;
- Les changements d'organisation ou d'activités à la demande de la direction générale ;
- L'évolution des exigences légales, réglementaires et contractuelles impactant le domaine d'application.

Amélioration continue

D'une manière générale, **l'ensemble du cycle de vie de la PSSI s'appuie sur le principe d'amélioration continue**, illustré par la roue de Deming (PDCA : Plan Do Check Act) ci-dessous :

SMSI : Système de Management de la Sécurité de l'Information



Phase	Action
PLANIFIER (PLAN)	Le RSSI établit la PSSI et sa déclinaison opérationnelle, validées par la Direction Générale. Il élabore ensuite un plan d'action, avec les directions concernées, permettant d'organiser l'implémentation des règles fixées. Ce plan d'action fait l'objet d'une validation de la Présidence et la direction générale des services.
RÉALISER (DO)	La PSSI est suivie par les directions impliquées, en s'appuyant sur les moyens fournis par le Responsable Informatique et son équipe.
CONTRÔLER (CHECK)	L'application des règles de la PSSI est contrôlée régulièrement à travers des audits et tests. Des indicateurs de sécurité (KPI) sont obtenus et analysés lors des comités de sécurité.
AJUSTER (ACT)	Les écarts relevés sont corrigés et/ou pris en compte pour la définition d'un nouveau cycle. Une nouvelle itération (PDCA) est effectuée.

Les thématiques de la PSSI

1. **Gouvernance :** Établir un cadre de gestion pour engager, puis vérifier la mise en œuvre et le fonctionnement de la sécurité de l'information au sein de l'organisation.

2. **Locaux informatiques :** Empêcher l'interruption des activités de l'organisation par la perte, l'endommagement, la destruction, le vol ou la compromission des actifs physiques.

3. **Ressources humaines :** S'assurer que les personnels sont sensibilisés et conscients de leurs responsabilités en matière de sécurité de l'information. Protéger les intérêts de l'établissement dans le cadre du cycle de vie des contrats de travail.

4. **Gestion des actifs :** Identifier les actifs de l'établissement et définir les responsabilités appropriées en matière de protection. S'assurer que l'information bénéficie d'un niveau de protection approprié conforme à son importance pour l'organisation.

5. **Accès logique :** Maîtriser l'accès utilisateur par le biais d'autorisations et empêcher les accès non autorisés aux systèmes et services d'information. Rendre les utilisateurs responsables de la protection de leurs informations d'authentification. Empêcher les accès non autorisés aux systèmes et aux applications.

6. **Accès privilégiés :** Maîtriser l'utilisation de privilèges élevés dans le contexte de l'Université. Rendre les utilisateurs responsables de l'usage de leurs accès privilégiés.

7. **Cryptographie :** Garantir l'utilisation correcte et efficace des techniques de cryptographie en vue de protéger la confidentialité, l'authenticité et/ou l'intégrité de l'information.

8. **Exploitation :** S'assurer de l'exploitation correcte et sécurisée des moyens de traitement de l'information. Garantir que l'information et les moyens de traitement de l'information sont protégés contre les logiciels malveillants. Empêcher toute exploitation des vulnérabilités techniques. Assurer l'horodatage et la traçabilité des actions, et en garantir la valeur probante. Empêcher la perte définitive de données.

9. **Réseaux et mobilité :** Garantir la protection de l'information circulant sur les réseaux, locaux ou étendus. Maintenir la sécurité de l'information en situation de mobilité, maintenir la sécurité de l'information transférée au sein de l'organisation et vers une entité extérieure.

10. **Sécurité dans les projets :** Veiller à ce que la sécurité de l'information soit prise en compte et mise en œuvre à tous les stades du cycle de vie des projets : conception, intégration, opérations et fin de vie.

Présidence

Direction Générale des Services
Pascale MONTELS
dgs@univ-rouen.fr

Mont-Saint-Aignan, le 30 septembre 2024

Monsieur Laurent YON
Président de l'Université de Rouen Normandie

À

Monsieur David CAUVIN

Objet : Lettre de mission « Responsable de la Sécurité des Systèmes d'Information »

Monsieur,

L'Université de Rouen Normandie vous a désigné Responsable de la Sécurité des Systèmes d'Information (RSSI) aux titres du décret n°2022-513 du 08 avril 2022[1] et de l'arrêté du 26 octobre 2022[2].

Au titre de votre qualité de Responsable de la Sécurité des Systèmes d'Information, vous êtes directement rattaché à la Direction Générale des Services et ne recevez aucune instruction pour l'exercice de vos missions.

1. Description de la mission

Dans le cadre de cette mission, il vous appartiendra de concevoir et d'animer la démarche sécurité : la disponibilité, l'intégrité, la confidentialité et la traçabilité des systèmes d'information (matériels, données et logiciels), et de faire respecter la politique de sécurité en veillant à ce que les niveaux de protections soient conformes à la réglementation et aux bonnes pratiques en matière de sécurité.

Au titre de vos fonctions, vous devrez :

- Identifier et formaliser les enjeux et les risques de sécurité majeurs pour l'établissement ;

[1] Décret n°2022-513 du 08 avril 2022 relatif à la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics
[2] Arrêté du 26 octobre 2022 portant approbation de l'instruction générale interministérielle n°1337/SGDSN/ANSSI sur l'organisation de la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics.

- Décliner les axes et les objectifs stratégiques en matière de cybersécurité et établir un plan d'actions pluriannuel recouvrant également les actions de sensibilisation et la promotion des « bonnes pratiques » ;
- Proposer à la gouvernance un plan d'actions préventives, correctives et prospectives en matière de sécurité SI en collaboration avec les parties prenantes (laboratoires, composantes, directions et équipes informatiques) ;
- Coordonner les différents intervenants en cas de problème (présidence, composantes, CERT, RENATER, autorités compétentes, sites extérieurs concernés, etc.) ;
- Exploiter et relayer les informations relatives à la sécurité reçues via le CERT, RENATER, CERTA, le FSSI/HFDS et/ou les correspondants sécurité de l'enseignement supérieur ;
- Définir une politique d'investissement au regard des objectifs de sécurité ;
- Analyser les besoins de sécurité des nouveaux projets, exprimés en termes de disponibilité, de confidentialité et d'intégrité des données, traçabilité ;
- Assurer la mise en conformité de l'établissement aux mesures et textes SSI réglementaires applicables ;
- Prévoir en liaison avec le délégué à la protection des données (DPD), la sensibilisation des usagers aux aspects de sécurité des données à caractère personnel ;
- Assurer la veille technologique et prospective pour garantir la sécurité logique et physique du SI ;
- Formaliser la stratégie de cyber-résilience tant pour la continuité (PCA) que pour la reprise d'activités (PRA) ;
- Tenir à jour un registre des incidents de sécurité liés au SI ;
- Organiser et formaliser un dispositif de gestion de crise sécurité ;
- Établir annuellement un rapport formalisé du niveau de couverture courant des risques de sécurité SI ;
- Assurer un rôle de conseil auprès de la gouvernance.

2. Responsabilités et obligations

Pour vous permettre de mener à bien ces différentes missions, vous serez amené à :

- Participer à des formations tant organisationnelles que techniques relatives à la sécurité des systèmes d'information ;
- Mener des actions de sensibilisation auprès du personnel et des usagers ;

- Organiser et animer un réseau de correspondants sécurité des systèmes d'informations (CSSI) au sein de l'Université de Rouen Normandie.

3. Durée de la mission

La mission est établie à compter du 1er Septembre 2024, pour la durée du mandat.

4. Moyens mis à disposition

Pour vous permettre de mener à bien ces différentes missions, la Direction s'engage à :

- Ce que vous soyez associé, d'une manière appropriée et en temps utile, à toutes les questions à la Sécurité du Système d'Information ;
- Vous aider à exercer vos missions en :
  - vous fournissant les ressources et moyens qui vous sont nécessaires ;
  - vous permettant d'entretenir vos connaissances spécialisées et vos capacités à accomplir vos missions, de réaliser votre veille et de vous tenir informé des meilleures pratiques propres à votre métier.
- Vous permettre de faire directement un rapport au niveau le plus élevé de la direction générale ;
- Donner une importance prépondérante à vos analyses et conseils en matière de Sécurité et, dans le cas où vos recommandations ne seraient pas retenues, à en documenter les raisons.

Je vous remercie par avance pour votre investissement dans la mise en œuvre de ces missions.

Je vous prie d'agréer, Monsieur, l'expression de mes salutations distinguées.

Le Président de l'Université de Rouen Normandie,

UNIVERSITÉ DE ROUEN NORMANDIE ★ 76821 Mont-Saint-Aignan Cedex ★

Laurent YON

Diffusion : DGS, DRH, DAJS, DSI