Politique de Sécurité du Système d'Information

version 1.4 28 avril 2025

Table des matières

I.Objectif

Ce document a pour but de décrire comment est déclinée la Politique de Sécurité des Systèmes d'information - PSSI - de l'État au sein de l'université d'Angers. Le document de référence est la version 1.0 du 17/07/2014 et approuvé par la circulaire du Premier ministre n° 5725/SG (NOR : PRMX1420095C) du 17 juillet 2014. Il est disponible en ligne sur le site institutionnel de l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI).

II. Contexte

A. STRUCTURATION

1. Généralités

L'Université d'Angers est un établissement public à caractère scientifique, culturel et professionnel. Les étudiants sont répartis sur 8 composantes :

- ESTHUA, Institut national de tourisme,
- UFR Santé,
- UFR des Sciences,
- UFR des Lettres, Langues et Sciences Humaines,
- IAE Angers-Cholet,
- IUT,
- Polytech Angers,
- UFR de Droit, d'Economie et de Gestion.

Implantée sur un territoire réputé pour la qualité de son cadre de vie, l'UA est installée au sein de 4 villes : Angers (3 campus : Belle-Beille, Saint-Serge et Santé), Cholet (1 campus), Saumur (1 campus) et les Sables-d'Olonne. Elle emploie des personnels (enseignants-chercheurs et personnels administratifs et techniques), et des intervenants professionnels qui assurent des vacations d'enseignement, ce qui fait d'elle le troisième employeur du territoire.

Les services centraux et les 6 services communs (Bibliothèque universitaire, service universitaire des activités physiques et sportives, service universitaire de l'information, de l'orientation et de l'insertion professionnelle, service universitaire de santé étudiante, service commun de l'alternance et de la formation professionnelle, service UA-Culture) participent au fonctionnement de l'établissement.

L'UA offre à sa communauté (étudiants, personnels administratifs, enseignants, chercheurs) des technologies et outils pédagogiques et scientifiques innovants ainsi que des infrastructures immobilières de qualité. Ces conditions permettent une vie étudiante riche et variée, une recherche fondamentale active et innovante ainsi qu'un des meilleurs taux de réussite en licence.

2. La Direction du Développement du Numérique

Au sein de l'Université d'Angers, la Direction du Développement Numérique (DDN) a en charge la gestion de tout l'environnement numérique de l'Université,

La DDN se compose des services suivants :

- Service Systèmes et Réseaux (SSR)
- Service des Usages du Numérique (SUN)
- Service Assistance et Moyens Informatiques (SAMI)
- Service d'appui à la pédagogie (Lab'UA)
- Service de la Transformation Numérique (STN), chargé de la coordination du SDN (écriture, mise en œuvre).

La cellule sécurité de la DDN rattachée à la direction de la DDN est composée de deux personnes, un RSSI et un ingénieur cybersécurité qui travaillent à temps plein.

3. Le SIEN

Les Universités ligériennes ont par ailleurs créé en 2021 un service mutualisé sous la forme d'un service général commun de type Service Inter Universitaire portant les projets d'un Datacenter labellisé, d'un réseau régional Très Haut Débit et d'Applicatifs mutualisés pour les acteurs de l'E.S.R en Région Pays de la Loire.

Ce service, de statut juridique Service Inter Universitaire porte le nom de "Service inter établissement Numérique" (cf. https://sien-pdl.fr)

Le SIEN ainsi créé est doté d'une gouvernance tripartite, chaque Université prenant la responsabilité de missions particulières au bénéfice de toutes. Il fonctionne en partenariat direct avec le Centre de Calcul (mésocentre) Régional pour l'E.S.R.

Il agit également au bénéfice des établissements partenaires de l'E.S.R qui le soutiennent : laboratoires (INSERM, CNRS, etc.), Écoles, Institutions (CROUS, Rectorat, etc.)

4. OR-Angers

Depuis 1999, l'Université d'Angers, et des établissements d'enseignement supérieur et de recherche de la Ville d'Angers (ESA, ESEO, UCO, Institut Agro, INRAE et le CROUS) ont créé le réseau métropolitain OR-Angers, infrastructure de fourreaux et de fibres optiques, à travers la Ville d'Angers, permettant la création de réseaux privés (licence L33-2 de la loi des télécommunications). L'université d'Angers assure l'exploitation de ce réseau métropolitain, au travers une licence L33-1.

OR-Angers se raccorde au réseau régional de l'enseignement supérieur et de la recherche (RRTHD-ESR-PDLL) piloté par le SIEN.

Plusieurs conventions délimitent le périmètre d'OR-Angers, conventions entre la Ville d'Angers et l'Université d'Angers, et, conventions entre les partenaires cités précédemment et l'université d'Angers. L'ensemble des conventions se terminent le 16 février 2034.

B. PÉRIMÈTRE

La Sécurité du Système d'Information (SSI) de l'Université d'Angers couvre la sécurité de l'ensemble des systèmes d'information de l'établissement avec toute la diversité que cela implique dans les usages, les lieux

d'utilisation, les méthodes d'accès, les personnes concernées, ...

On peut citer de manière non exhaustive :

- Le système informatique de gestion ;
- Les applications de communications (messagerie, applications et publications Internet, bureautique, ...) ;
- Les applications liées à l'enseignement et la recherche ;
- Les systèmes adossés aux supports ou échanges des ressources numériques (stockage, sauvegarde, ToIP/VoIP, visioconférence, vidéosurveillance, contrôle d'accès, ...) ;
- Les interconnexions avec les autres organismes de tutelles (ex : CNRS, INSERM).

C. PILOTAGE

Au sein de l'Université d'Angers, la responsabilité générale de la sécurité des systèmes d'information relève du Président de l'université en tant qu'Autorité Qualifiée pour la Sécurité des Systèmes d'Information (AQSSI). Il est assisté dans cette fonction par le Responsable de la Sécurité des Systèmes d'Information (RSSI).

La PSSI de l'Université d'Angers s'inscrit dans le cadre de la politique et des directives émanant de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), en charge de la sécurité des systèmes d'information au niveau national. Cette politique et ces directives sont relayées, par le Haut Fonctionnaire de Défense et de Sécurité (HFDS) du ministère de l'éducation nationale, de l'enseignement supérieur et de la recherche et par le Fonctionnaire de Sécurité des Systèmes d'Information (FSSI) placé auprès de lui.

D. INTÉGRATION AU CYCLE DE VIE DU SI

Tout système d'information devrait faire l'objet d'une décision d'homologation de sa sécurité avant sa mise en exploitation dans les conditions d'emploi définies. L'homologation est l'acte selon lequel l'autorité atteste formellement auprès des utilisateurs que le système d'information est protégé conformément aux objectifs de sécurité fixés.

La sécurité du SI doit être prise en compte dans toutes les phases des projets comportant un volet numérique, de la conception et de la spécification du système jusqu'à son retrait du service.

III. Mise en œuvre de la PSSI

A. ORGANISATION, RESPONSABILITÉS

1. Responsabilités des différents acteurs

La présente PSSI concerne l'ensemble des personnes physiques ou morales utilisatrice du SI de l'Université d'Angers, qu'il s'agisse des agents de l'établissement ou de tiers (prestataires ou sous-traitants).

2. Responsables SSI

Le RSSI assure les missions attendues par l'ANSSI. Le RSSI assure le pilotage de la démarche de cybersécurité de l'UA. Il définit la politique de sécurité des systèmes d'information (prévention, protection, détection, résilience, remédiation) et veille à son application. Il assure un rôle de conseil, d'assistance, d'information, de formation et d'alerte. Il s'assure de la mise en place des solutions et des processus opérationnels pour garantir la protection des données et le niveau de sécurité des systèmes d'information.

La cellule sécurité de la DDN est en lien constant avec tous les services de la DDN. Elle est également chargée du traitement des alertes identifiées par RENATER, le CERT-FR et l'ANSSI" et des alertes détectées en interne. Elle rend compte des incidents auprès du CERT RENATER. Elle est chargée de la réalisation d'audits internes et participe de manière opérationnelle à la mise en œuvre de la PSSI d'établissement.

Des correspondants SSI sont identifiés et participent aux projets concourant à l'amélioration de la sécurité du SI.

L'approche par projet permet de faire intervenir d'autres acteurs, non identifiés comme correspondant SSI, experts dans le domaine concerné.

Une cellule de crise SSI est activable à tous moments (cf annexe Processus de mobilisation de la cellule de crise.

3. Chartes informatiques et guide technique

Toute personne utilisant les moyens informatiques de l'Université d'Angers doit reconnaître au préalable la "*charte d'usage du système d'information*" intégrée au règlement intérieur de l'établissement (Titre 8).

Celle-ci formalise de nombreuses dispositions de la PSSI de l'État.

La charte est complétée par le "*guide technique de l'utilisateur du SI*" qui a pour objet de définir les procédures techniques devant être appliquées par toute personne utilisant les moyens informatiques et de télécommunications de l'université d'Angers.

Les membres de la DDN concernés doivent respecter la charte d'"*Engagement éthique et déontologique de l'administrateur systèmes, réseaux et de système d'informations*".

Une charte d'engagement est à valider pour les utilisateurs qui souhaitent être administrateur de leur poste de travail.

4. Cyber surveillance

La Direction du Développement du Numérique utilise plusieurs outils pour tenter de repérer les activités qui semblent suspectes au regard de la sécurité du SI
Les dispositifs mis en place sont conformes à la réglementation en vigueur. Ils respectent les principes de proportionnalité et de transparence.

5. Gestion des prestataires

Le guide des clauses de sécurité (en annexe) à intégrer à tout marché d'achat de prestation ou d'outil numérique fixe les règles à suivre. Il précise entre autres les obligations pour les titulaires manipulant des informations de l'université d'Angers sur leur SI.

B. SÉCURITÉ DES RÉSEAUX

1. Equipements d'interconnexion

Dans l'ensemble des locaux de l'établissement, les équipements d'interconnexion (commutateurs, routeurs, points d'accès WiFi, etc..) sont sous la responsabilité du Service Systèmes et Réseaux (SSR) de la Direction du Développement du Numérique (DDN). Afin de protéger le système d'information de l'établissement, tout équipement d'interconnexion non administré par le SSR de la DDN doit faire l'objet d'une validation du RSSI d'une part et de la DDN d'autre part.

Ces équipements disposent d'une interface de gestion dédiée dont l'accès est restreint aux seuls administrateurs systèmes et réseaux concernés. Cette interface de gestion n'est pas donc exposée aux usagers du système d'information et une authentification sécurisée est nécessaire pour y accéder.

Les équipements d'interconnexion, sauf points d'accès WiFi, sont installés dans des locaux à accès restreint limités aux services concernés par la maintenance de ces équipements ou de ces locaux (services de DDN, de la DPIL et service de maintenance des bâtiments des composantes concernés).

La configuration de chacun de ces équipements est sauvegardée et journalisées sur les systèmes de gestion centralisés dédiées.

2. Sécurité des réseaux WiFi

Les réseaux WiFi sont par nature plus exposés à une intrusion extérieure. Le niveau de sécurité le plus élevé possible est mis pour chacun d'entre eux.

Pour l'accès des usagers, l'accès via le réseau eduroam est privilégié. Ce réseau utilise une authentification basée sur le protocole 802.1x et l'infrastructure de serveurs RADIUS du projet eduroam (https://eduroam.org/). Une segmentation de réseau est mise en place afin de séparer les différents usagers et limiter ainsi l'exposition en cas d'intrusion.

Pour les besoins complémentaires, type IoT par exemple, une authentification par clé PSK est mise en place avec un filtrage par adresse MAC. Sur les réseaux de ce type les plus sensibles, la clé est renouvelée une fois par an. Ces clés sont partagées entre le SSR et les responsables des équipements clients de ces réseaux. Ces réseaux ne transportent aucune donnée sensible.

Pour le bon fonctionnement de l'infrastructure WiFi, la diffusion de réseaux WiFi par d'autres équipements est interdite.

L'ensemble de ces accès est journalisé et conservé dans le service de journalisation centralisé de la DDN selon un délai indiqué dans la charte d'usage du système d'information.

Le comportement inadapté d'un équipement ou d'un usager peut entraîner le blocage de ses accès aux réseaux WiFi proposés par l'établissement.

3. Sécurité des réseaux filaires

Les réseaux filaires sont segmentés en sous-réseaux afin de séparer les différents équipements constitutifs du système d'information de l'établissement. Cette segmentation permet de séparer des ensembles de services en fonction de la criticité des données qu'ils traitent, de la population y nécessitant un accès, de l'évaluation du risque de sécurité liés à ces services (maintenabilité du système d'exploitation, du service, etc.).

Une protection renforcée est mise en place concernant la création de boucles et le raccordement d'un serveur DHCP illégitime en particulier sur les sous-réseaux de raccordement de postes de travail et d'équipements de type BYOD.

4. Sécurité avec Internet

Les accès depuis Internet vers les réseaux publics de l'établissement sont limités aux services utiles déclarés à la DDN.

Les accès vers Internet pour l'ensemble des réseaux internes de l'établissement sont filtrés, journalisés et analysés afin de se limiter aux flux légitimes utiles au fonctionnement des équipements de ces réseaux.

5. Sécurité de la commutation et du routage

La communication entre les sous-réseaux de l'établissement transite au travers du système de pare-feu de l'établissement qui n'autorise que les flux explicitement nécessaires. Tout trafic numérique non explicitement autorisé est alors interdit. Les flux sont étudiés à chaque mise en place d'un nouveau service et doivent faire l'objet d'une revue régulière. Le pare-feu de l'établissement est placé sous la responsabilité du SSR.

L'ensemble du trafic est journalisé et conservé dans le service de journalisation centralisé de la DDN selon un délai indiqué dans la charte d'usage du système d'information.

Ce trafic est aussi remonté à un système d'analyse de menace afin de détecter les activités nuisibles et limiter au plus vite la propagation d'activités malveillantes.

Les équipements de routage utilisent des mécanismes robustes et sécurisés permettant de limiter l'injection de données de routage malveillantes.

C. PROTECTION DES DONNÉES

1. Disponibilité, confidentialité

Les données des utilisateurs sont hébergées sur une infrastructure de stockage haute disponibilité avec un premier niveau de redondance local et un second niveau de redondance géographique. Cela permet de garantir un temps de coupure annuel minimal.

Un second niveau de garantie d'accès aux données est assuré par la solution de sauvegarde qui permet de la restauration multi-temporelle. Cette solution garantit également une sauvegarde sur support externe des données les plus sensibles afin qu'elles ne soient plus en ligne et directement accessibles.

La confidentialité des données est assurée par la mise en œuvre de politiques de sécurité qui gèrent les droits d'accès des utilisateurs et des accès aux ressources.

2. Protection des données sensibles

Les données sensibles sont hébergées sur des systèmes hautement redondants. Ces systèmes sont eux même opérés dans des environnements sécurisés que ce soit en termes d'alimentation électrique, de gestion de la température et de l'hygrométrie ou encore des accès physiques.

Notre Datacenter respecte les recommandations Tier III tel que préconisées pour les centres de données sensibles.

3. Hébergement externe

Toute opération d'externalisation s'appuie sur une analyse de risques préalable, de façon à formaliser des objectifs de sécurité et définir des mesures adaptées. L'ensemble des objectifs de sécurité ainsi formalisés permet de définir une cible de sécurité servant de cadre au contrat établi avec le prestataire.

Tout contrat d'hébergement détaille les dispositions mises en œuvre pour prendre en compte la SSI. Ce sont notamment les mesures prises pour assurer le maintien en condition de sécurité des systèmes et permettre une gestion de crise efficace (conditions d'accès aux journaux, mise en place d'astreintes, etc.).

Le document "Guide des clauses de sécurité à intégrer aux achats" présent en annexe précise les attendus à décrire lors des procédures d'achat de services d'hébergement externe.
Pour tous services d'hébergement externe, qui ne feraient pas l'objet de procédure d'achat, il conviendra de se rapprocher des exigences attendues d'un potentiel titulaire d'une procédure d'achat.

D. EXPLOITATION SÉCURISÉE DES RESSOURCES INFORMATIQUES

1. Administration des serveurs

L'administration des serveurs internes de l'établissement hébergeant les briques principales du SI est placée sous la responsabilité des administrateurs systèmes et réseaux du SSR de la DDN.

2. Administration des postes de travail

L'administration des postes de travail individuels est placée sous la responsabilité des agents du SAMI. Ces postes peuvent être fixes ou nomades.

L'administration des postes par les utilisateurs eux-mêmes doit demeurer l'exception et être justifiée en termes de besoins et de compétences. Une charte d'engagement de l'administrateur local doit être signée par l'utilisateur qui souhaite administrer son poste.

Les agents du SAMI et de la cellule de sécurité du SI peuvent intervenir à distance pour des opérations de maintenance sur le poste de travail d'un utilisateur après l'en avoir averti et obtenu son consentement, en respectant les principes de la loi Informatique et Libertés.

3. Sécurisation des postes de travail

Un outil de type EDR (Endpoint Detection and Response) a été déployé depuis avril 2023. Il est recommandé de l'activer sur l'ensemble des postes des personnels.

Chaque poste de travail requiert l'authentification nominative de l'utilisateur. S'il a signé la charte de

l'administrateur un compte spécifique d'administration lui est créé et ne sert qu'aux opérations d'installation/configuration, aucunement pour l'usage quotidien.

Chaque poste de travail est inventorié et suivi dans notre base de gestion de parc.

Les mises à jour de sécurité des OS de chaque poste de travail sont appliquées automatiquement.

Les bonnes pratiques de configuration recommandées par le constructeur, notamment le renforcement du système d'exploitation, doivent être appliquées sur tous les postes, et tout particulièrement sur ceux utilisés par les administrateurs de serveurs ou d'équipements sensibles, où les exigences de sécurité sont encore plus strictes.

Les postes de travail ne doivent pas stocker de données sensibles.

4. Sécurisation des serveurs

Un outil de type EDR (Endpoint Detection and Response) a été déployé depuis avril 2023. Il est recommandé de l'activer sur l'ensemble des serveurs administrés par la DDN.

Chaque serveur dispose d'une interface de gestion dédiée. Un compte d'administration nominatif et spécifique est nécessaire pour accéder aux fonctionnalités d'administration. Un compte est créé pour chaque administrateur nécessitant un accès. Les interfaces de gestion des serveurs sont positionnées dans des sous-réseaux dont l'accès est limité aux seuls postes d'administration des administrateurs du serveur et des applications hébergées.

Les mises à jour sont appliquées régulièrement en qualifiant au préalable l'impact des celles-ci sur le bon fonctionnement des services hébergés.

Les journaux applicatifs et systèmes sont transférés vers le service de journalisation centralisé de la DDN. Ils font l'objet d'analyses et sont conservés selon un délai indiqué dans la charte d'usage du système d'information.

Ces serveurs sont sauvegardés régulièrement.

5. Gestion des authentifiants

Se référer à la "*charte d'usage du système d'information*" où ils sont nommés "*codes d'accès*".

Toute action d'autorisation d'accès d'un utilisateur à une ressource du SI, doit s'inscrire dans le cadre d'un processus d'autorisation formalisé, qui s'appuie sur le processus d'arrivée et de départ d'une personne.

6. Sécurité des applications

Les applications manipulant des données sensibles doivent permettre une gestion fine par profils d'accès. Les principes du besoin d'en connaître et du moindre privilège s'appliquent.

Tout déploiement d'application doit être accompagné d'un dossier précisant les outils, stratégies, méthodes et/ou mesures mises en place pour sécuriser ladite application, en tenant compte tout particulièrement de la sensibilité des données exploitées par cette application.

Le dossier de sécurité doit être présenté au RSSI pour validation.

7. Infogérance et télémaintenances externes

L'infogérance et/ou la télémaintenance externe supposent de donner accès au SI de l'Université d'Angers à une société extérieure, que cet accès se fasse à distance ou physiquement depuis les locaux de

l'établissement.

Dans ce cas de figure, un contrat entre l'Université et le prestataire intervenant doit encadrer précisément les droits d'accès octroyés au prestataire, les modalités de ses interventions, les engagements et imputabilité de responsabilité en cas d'incident.

Tout mécanisme permettant de vérifier le respect des limites d'interventions indiquées dans ce contrat doit être mis en place.

L'externalisation (infogérance, télémaintenance) d'éléments critiques du SI est à éviter. Si cette externalisation est inévitable, elle doit se voir adjointe des garanties spécifiques demandées au prestataire, puis être validée par le RSSI.

8. Accès à distance au SI

Le système d'information de l'UA peut être accédé à distance au travers de la plateforme VPN administrée par la DDN. Un accès nominatif et profilé est mis à disposition en fonction des besoins des utilisateurs, qu'il s'agisse de personnels de l'établissement ou de prestataires externes.

Les règles et recommandations quant à son utilisation sont décrites dans le guide technique de l'utilisateur du SI.

9. Maintien du niveau de sécurité

L'université met en œuvre des procédures garantissant un maintien du niveau de sécurité de ses ressources informatique. Cela inclut l'application des mises à jour, la surveillance proactive des infrastructures, la correction rapide des vulnérabilités identifiées et la suppression des systèmes d'exploitation obsolètes.

Des audits de sécurité sont réalisés régulièrement, accompagnés d'une vérification périodique de la documentation.
Des mesures complémentaires, par exemple le renouvellement périodique des mots de passe, viennent renforcer la sécurité des accès.

E. MESURE DU NIVEAU EFFECTIF DE SÉCURITÉ

1. Contrôle de gestion

Un tableau de bord de la SSI construit sur la base des indicateurs de la PSSI de l'État est actualisé tous les ans.

Il est communiqué sur demande et si les destinataires sont habilités à en connaître.

2. Audits réguliers

La cellule de sécurité informatique, par l'utilisation d'outils adaptés aux différents domaines sensibles (Active Directory, sites web publics, ...) réalise régulièrement des audits de sécurité afin de vérifier le niveau de protection du SI.

Des prestations externes peuvent être sollicitées en complément afin de mettre à contribution des experts dans des domaines à investiguer plus précisément.

3. Journalisation, fichiers de traces, logs

Une journalisation des logs applicatifs est effectuée et un système de centralisation permet d'agréger toutes les informations afin de proposer un requêtage croisé. Ce type de requêtage autorise une analyse fine de tout ce qui se passe au sein du SI de l'université d'Angers au travers de l'exploitation de la corrélation des évènements.

La durée de conservation de ces journaux est indiquée dans la charte d'usage du système d'information.

4. Gestion d'incidents

En cas d'incident de sécurité, l'université déclenche une procédure structurée comprenant les étapes de détection, d'analyse, de réponse et de résolution. La cellule de sécurité, composée du RSSI et de l'ingénieur cybersécurité, pilote ce processus. Toutes les actions menées dans le cadre de la gestion de l'incident sont documentées pour assurer un suivi précis et améliorer les mesures de prévention futures.

En cas d'incident de sécurité critique, la cellule de crise est activée conformément à la procédure décrite dans le document intitulé "Mobilisation de la cellule opérationnelle de crise PCA numérique".

5. Gestion de crise / plan de continuité

L'université d'Angers dispose d'un plan de continuité d'activité numérique définissant la manière dont les outils numériques et informatiques peuvent être maintenus en mode dégradé et/ou restauré dans leurs fonctions maximales d'efficience en cas d'attaque de type cyber.

F. ANNEXE

1. Liste des documents référencés

- Charte d'usage du système d'information de l'université d'Angers au titre 8 du Règlement Intérieur
- Guide technique de l'utilisateur du système d'information
- Engagement éthique et déontologique de l'administrateur
- Engagement de l'administrateur local de son ordinateur
- Guide des clauses de sécurité à intégrer aux achats de sécurité à intégrer aux achats
- Processus de mobilisation de la cellule de crise