CONSEIL D'ADMINISTRATION
DELIBERATION N° 2018-07-06-24

DELIBERATION DU CONSEIL D'ADMINISTRATION DE L'UNIVERSITE CLERMONT AUVERGNE PORTANT APPROBATION DE LA POLITIQUE DE SECURITE DES SYSTMES D'INFORMATION

LE CONSEIL D'ADMINISTRATION DE L'UNIVERSITE CLERMONT AUVERGNE, EN SA SEANCE DU 06 JUILLET 2018,

Vu le code de l'Education ;
Vu les statuts de l'Université Clermont Auvergne ;
Vu l'avis du comité technique de l'UCA du 25 juin 2018 ;

PRESENTATION DU PROJET

La Sécurité des Systèmes d'Information (SSI) est une préoccupation majeure de notre établissement. Cette démarche est d'autant plus d'actualité que la réglementation évolue avec la mise en application, à partir du 25 mai 2018 du Règlement Général de la Protection des Données (RGPD). Ce nouveau Règlement consacre et renforce les grands principes de la loi Informatique et Libertés, en vigueur depuis 1978, et accroît sensiblement les droits des citoyens en leur donnant plus de maitrise sur leurs données.

Le périmètre à couvrir en matière de SSI touche aussi bien les outils numériques que les données elles-mêmes de l'administration, de la recherche et de la pédagogie et concerne tous les utilisateurs. L'approche se fait selon 3 critères fondamentaux, la Disponibilité, L'Intégrité et la Confidentialité.

Afin de donner un cadre de référence à la démarche SSI, nous vous soumettons trois documents fondamentaux:

La Politique de Sécurité des Systèmes d'information (PSSI).
La PSSI est élaborée et sa mise en œuvre est contrôlée par le Comité de Pilotage SSI (CPSSI) composé de l'Autorité Qualifiée SSI (le Président ou son représentant le VP numérique), du Directeur Général des Services, du Fonctionnaire Sécurité de Défense, du Directeur des Systèmes d'Information, du Responsable de la Sécurité des Systèmes d'Information et de ses suppléants, du Délégué à la Protection des Données et éventuellement d'experts suivant les thématiques abordées.
La PSSI est la pierre angulaire de la démarche SSI au sein de l'établissement. Elle repose sur deux normes ISO principales (ISO 27001 et 27002). La première traduit les objectifs en matière d'organisation, de pilotage, de management, de qualité, de sensibilisation à la SSI. La seconde, plus technique, décline les bonnes pratiques à mettre en œuvre pour l'atteinte des objectifs.
La PSSI présente un volet politique décliné suivant différents domaines techniques et un volet opérationnel qui donne une liste de livrables à élaborer suivant un plan d'action.
Elle est donc un cadre de référence pour les personnels informaticiens quel que soit le métier (développeur, administrateur de Systèmes d'Information, ingénieur infrastructure, technicien de proximité, etc)

La Charte des administrateurs techniques.
C'est est un des livrables mentionnées dans la PSSI. Elle définit les droits et les devoirs des administrateurs de ressources informatiques que ce soit du point de vue de l'infrastructure (essentiellement les serveurs et le réseau) des logiciels ou des données.

La politique de gestion des journaux informatiques.
Ce document est un autre livrable de la PSSI. Il fixe les modalités d'enregistrement et le cadre d'utilisation des journaux informatiques. Ces derniers retraçant une partie de l'activité sur le système d'information et les ressources de façon à :
- répondre aux contraintes légales en cas de réquisition par l'autorité judiciaire

- répondre quotidiennement aux enjeux de sécurité et de disponibilité des services numériques offerts aux utilisateurs
- élaborer des statistiques à des fins de qualité

Vu la présentation de Monsieur le Président de l'université Clermont Auvergne ;

Après en avoir délibéré ;

DECIDE

d'approuver la Politique de Sécurité des Systèmes d'information (PSSI), la charte des administrateurs techniques et la politique de gestion des journaux informatiques tels que joints en annexe.

Membres en exercice : 37
Votes : 24
Pour : 24
Contre : 0
Abstentions: 0

Le Président,

Mathias BERNARD

CLASSE AU REGISTRE DES ACTES SOUS LA REFERENCE : CA UCA 2018-07-06-24

TRANSMIS AU RECTEUR :

PUBLIE LE :

Modalités de recours : *En application de l'article R421-1 du code de justice administrative, le Tribunal Administratif de Clermont-Ferrand peut être saisi par voie de recours formé contre les actes réglementaires dans les deux mois à partir du jour de leur publication et de leur transmission au Recteur*.

UNIVERSITE CLERMONT AUVERGNE

POLITIQUE DE SECURITE DU SYSTEME D'INFORMATION

DECEMBRE 2017

UNIVERSITÉ
Clermont
Auvergne

Avertissement

La version initiale de ce document a été réalisée par la société FIDENS dans le cadre du marché « Fourniture d'une PSSI générique pour les établissements d'enseignement supérieur et d'une boite à outil permettant son adaptation »

FIDENS SA

8-10, rue Emile Sehet

95157 Taverny cedex

1. Avant-propos

1.1. Objectifs de la PSSI

[ISO 27001 - A 5.1.1]	Document de politique de sécurité de l'information

La Politique de Sécurité des Systèmes d'Information est le document de référence pour l'Établissement, qui énonce les règles opérationnelles de sécurité qui doivent être implémentées. Ces règles découlent des mesures sélectionnées en réponse aux risques évalués sur l'ensemble du périmètre de l'Établissement.

La Politique de Sécurité des Systèmes d'Information de notre établissement est adossée à la Politique de Sécurité des Systèmes d'Information de l'Etat – dite PSSIE – dans un objectif de convergence vers les préconisations ministérielles.

Logique rédactionnelle

Les règles de sécurité décrites dans la PSSI sont ordonnées et référencées selon les thèmes ISO-27002:2005 (ou annexe A ISO-27001:2005) afin de faciliter la gestion des risques, leur suivi de mise en œuvre et la conduite éventuelle d'audit du SI ou SMSI conformément à l'ISO-27001:2005.

La ou les mesures de l'annexe A de la norme ISO-27001:2005 sont rappelées en encadré au-dessus de la ou des règles de sécurité plus précises définies par la PSSI, comme c'est le cas en tête de ce paragraphe.

1.2. Périmètre

La PSSI s'applique à l'ensemble du système d'information de l'Établissement et à ses ressources hébergées au sein des différentes structures de la DSI.

Par "Système d'Information", il faut comprendre l'ensemble des moyens mis en œuvre par l'Établissement pour opérer les services nécessaires à ses missions et qui traitent les informations de Gestion, d'Enseignement et de Recherche. Ainsi, au-delà des matériels informatiques, des logiciels et des données manipulées, la PSSI définit aussi des règles de sécurité relatives à l'organisation, aux personnes opérant ces systèmes et à leurs infrastructures d'accueil.

2. Gestion de la politique de sécurité

2.1. Organisation pour la gestion de la SSI

Un Comité de Pilotage de la Sécurité des Systèmes d'Information (CPSSI) est mis en place, afin de coordonner les activités liées à la sécurité, et de veiller à sa mise en œuvre au sein de l'Etablissement.

2.2. Mise en œuvre de la politique de sécurité

La présente Politique de Sécurité est rédigée sous la responsabilité du Comité de Pilotage de la Sécurité des Systèmes d'Information (CPSSI).

La mise en œuvre opérationnelle des règles, par les différentes catégories de personnels, peut être appuyée par des documents d'application dont la liste est établie en annexe du présent document.

2.3. Approbation et Diffusion

La PSSI est approuvée par le Président en sa qualité d'Autorité Qualifiée de la Sécurité des Systèmes d'Information (AQSSI). C'est un document à diffusion restreinte à l'établissement et à certains de ses partenaires. Elle est diffusée à tout le personnel de l'établissement ayant le besoin d'en connaître le contenu. Elle est présentée devant le CA de l'Université CLERMONT AUVERGNE.

2.4. Contrôle et suivi

La PSSI sert de référentiel aux audits internes de la Sécurité des Systèmes d'Information. A ce titre, les manquements ou défauts d'implémentation sont identifiés et analysés par le CPSSI.

2.5. Gestion des évolutions

[ISO 27001 - A 5.1.2]	Réexamen de la politique de sécurité de l'information

Le CPSSI procède annuellement à la mise à jour de la PSSI en fonction des évolutions du système d'information, des besoins de sécurité, et des risques nouveaux identifiés.

Le président de l'établissement, en tant que Autorité Qualifiée de la Sécurité des Systèmes d'Information (AQSSI), approuve la version finalisée du document.

2.6. Relations avec les autorités

ISO 27001 - A 6.1.6]	Relations avec les autorités

[GPS_01] Relations avec les autorités compétentes

La gestion de la sécurité doit couvrir et définir les relations à établir avec les autorités compétentes et notamment sur les aspects suivants :

- Respect des lois et réglementations
- Remontées en cas d'incidents de sécurité grave (vers le CERT-Renater voire l'ANSSI)
- Gestion des données personnelles (CNIL)

3. Orientations générales

3.1. Lignes directrices

L'établissement se doit de protéger son patrimoine informationnel face aux risques pouvant impacter ses orientations stratégiques, ou pouvant affecter la réalisation de ses missions. La PSSI doit concourir à l'atteinte des objectifs de l'Etablissement à savoir permettre un développement de ses activités d'enseignement et de recherche localement, au national et à l'international notamment en ce qui concerne le volet numérique.

Elle doit restreindre les possibilités d'utilisation du réseau internet et des moyens de l'Université d'une façon compatible avec la nécessaire créativité qui accompagne les activités de l'établissement

La PSSI doit être compatible avec les exigences légales notamment dans les domaines suivants :

- Informatique et liberté
- Sécurité intérieure
- Propriété intellectuelle
- E-administration
- Cybercriminalité – Internet
- Éducation – Recherche

3.2. Actions de sensibilisation.

La sensibilisation des personnes à la sécurité de l'information constitue un maillon essentiel de la sécurité. Ainsi, le service des Ressources Humaines organise régulièrement des sessions de formation ou de sensibilisation adaptées aux besoins des différents usagers : agents, chercheurs enseignants, étudiants, personnels des services informatiques, en coopération avec la DSI et sous la responsabilité du RSSI. Un plan annuel de sensibilisation est proposé par le CPSSI.

4. Gestion des biens

4.1. Classification des biens

[ISO 27001 - A 7.2.1]	Lignes directrices pour la classification

[GDB_01] Plan de classification

Un plan de classification est défini au niveau de l'établissement pour différencier les biens sensibles des éléments ordinaires du système d'information. Ce plan de classification définit les échelles de sensibilité à partir des critères confidentialité, intégrité, et disponibilité.

4.2. Inventaire des biens

[ISO 27001 - A 7.1.1]	Inventaire des biens

[GDB_02] Identification et inventaire des biens sensibles

Les biens sensibles participant au fonctionnement du système d'information (informations, biens logiciels, biens physiques, services, etc.) sont inventoriés par domaine. Chaque bien recensé fait l'objet d'une identification renseignant le niveau de classification (établi sur la base du plan mentionné ci-dessus), son détenteur ou responsable, et les personnes qui y ont accès (pour les données).

La réalisation de cet inventaire est à la charge de la DSI ou des structures locales.

4.3. Marquage des biens

[ISO 27001 - A 7.2.2]	Marquage et manipulation de l'information

[GDB_03] Marquage des biens

Tous les biens matériels seront identifiés par leurs étiquettes d'inventaire comptable UCA.

4.4. Propriété des biens

[ISO 27001 - A 7.1.3]	Utilisation correcte des biens

[GDB_04] Utilisation des biens

Tout matériel n'appartenant pas à l'établissement et n'étant pas géré par les équipes d'exploitation du SI est considéré comme un composant externe (PC, clé USB, équipement réseau,…).

Hors ressources suivantes validées par la DSI (wifi et réseaux dédiés aux « invités »), aucune connexion de matériels externes au réseau interne de l'établissement n'est autorisée sauf accord du responsable informatique local en conformité aux règles définies par la présente PSSI. Tout matériel appartenant à l'Établissement et géré par les équipes d'exploitation du SI respecte les règles d'exploitation définies par la DSI. En particulier, les droits d'administration pour les utilisateurs ne sont pas autorisés sauf accord, des administrateurs informatiques locaux.

5. Sécurité liée aux ressources humaines

5.1. Responsabilités des utilisateurs

[ISO 27001 - A 8.1.1]	Rôles et responsabilités

[PER_01] Responsabilités génériques

La charte du numérique et les livrables associés ou documents connexes (dont chartes spécifiques) précisent les droits, devoirs et responsabilités qui incombent à tout utilisateur du système d'information en matière de sécurité :

- Règles d'utilisation des outils (postes de travail bureautiques ou nomades) et des services génériques (messagerie, Intranet…) mis à la disposition de chacun.
- Règles de protection des biens.
- Responsabilités de l'utilisateur vis-à-vis de la sécurité.

[ISO 27001 - A 6.1.3]	Attribution des responsabilités en matière de sécurité de l'information

[PER_02] Responsabilités spécifiques et postes de confiance

Le CPSSI détermine des fonctions de confiance et identifie les personnels assurant ces fonctions. Celles-ci sont confiées à des personnels qualifiés et formés à la sécurité.

[ISO 27001 - A 6.1.5]	Engagements de confidentialité

[PER_03] Confidentialité des données

Le respect de la confidentialité des données est rappelé dans a charte du numérique afin que toute personne pouvant avoir accès à des informations sensibles soit tenue à leur non divulgation en dehors des procédures de travail.

[ISO 27001 - A 8.2.3]	Processus disciplinaire

[PER_04] Manquement aux exigences

La charte du numérique définit les conditions d'usage du système d'information en termes de sécurité. Elle informe les utilisateurs que des contrôles peuvent être effectués et mentionne le processus disciplinaire (rappel aux bonnes pratiques, sanction administrative, poursuite pénale…) mis en œuvre en cas de d'infraction aux règles de sécurité.

5.2. Sélection des personnels

[ISO 27001 - A 8.1.2]	Sélection

[PER_05] Prise en compte de la sécurité dans la sélection des personnels

L'aptitude à respecter, définir et mettre en œuvre les règles de sécurité est prise en considération lors du recrutement du personnel sur des postes d'informaticien (BAP E).

5.3. Formation et sensibilisation du personnel et des usagers

[ISO 27001 - A 8.2.2]	Sensibilisation, qualification et formations en matière de sécurité

[PER_06] Information du personnel et des usagers

La charte du numérique, accessible sur le site web institutionnel, informe chaque membre du personnel des consignes de sécurité à respecter.

L'information de sécurité concerne à la fois les personnels de l'établissement (personnels administratifs, les enseignants, les chercheurs), mais aussi les étudiants, tiers et contractants.

[PER_07] Sensibilisation des personnels

Il est important que chaque personne impliquée dans le traitement d'informations sensibles de l'établissement soit sensibilisée aux enjeux de « sécurité » et soit formée de manière à pouvoir gérer les mesures de sécurité qui lui incombent.

Des sessions d'information à la sécurité sont assurées périodiquement, éventuellement en E-learning, afin de garantir la vigilance des personnels administratifs, enseignants, chercheurs et étudiants, sur les bonnes pratiques de sécurité ou sur les règlements en vigueur.

Des éléments de formation spécifique sont réalisés pour les personnels dont les fonctions requièrent une sensibilisation particulière en termes de sécurité (informaticiens et gestionnaires).

5.4. Disponibilité des personnels critiques

[ISO 27001 - A 6.1.1]	Engagement de la direction vis-à-vis de la sécurité de l'information

[PER_08] Disponibilité des personnes critiques

Une gestion adaptée des ressources humaines est mise en place de manière à ce qu'il n'y ait pas de vacance sur un poste critique qui puisse impacter la sécurité, ou induire une indisponibilité incompatible avec les objectifs de sécurité retenus. Il convient en particulier que les ressources affectées soient en cohérence avec les objectifs en matière de disponibilité. Les postes critiques portant un risque en termes de continuité d'activité devront être si possible doublonnés, identifiés et répertoriés

5.5. Suivi des biens, ressources et autorisations allouées

[ISO 27001 - A 6.1.4]	Système d'autorisation concernant les moyens de traitement de l'information

[PER_09] Gestion des biens et autorisations alloués aux personnes

Les biens sensibles (badges, équipements…) et les autorisations (accès aux locaux, aux données et fonctions du SI…) alloués à chaque personne sont gérés et suivis.

6. Gestion des tiers

[ISO 27001 - A 6.2.1]	Identification des risques provenant des tiers

[TIERS_01] Identification des risques liés aux relations avec des tiers

Toute interconnexion entre le SI de l'établissement et le SI d'un tiers (ou d'un laboratoire) se fait en conformité avec les règles édictées par la DSI. Toute demande spécifique fait l'objet d'une étude pour valider les besoins, identifier les risques, et définir les mesures de sécurité complémentaires à mettre en œuvre par l'établissement ou par le tiers.

[ISO 27001 - A 6.2.2]	La sécurité et les clients

[TIERS_02] Sécurité liée aux accès clients

Lorsqu'une relation de type client / fournisseur est établie entre l'établissement et un organisme ou une personne externe (échanges d'informations avec des laboratoires, avec des étudiants), les besoins de sécurité sont étudiés par le gestionnaire du bien. Cette étude se fait avec l'appui du RSSI et de la DSI, avant l'ouverture d'un accès à l'information ou aux biens de l'établissement.

[ISO 27001 - A 6.2.3]	La sécurité dans les accords conclus avec des tiers

[TIERS_03] Prise en compte de la sécurité dans les relations contractuelles

Des accords de confidentialité et annexes de sécurité spécifiant les éléments couverts par ces accords sont établis dès les phases précontractuelles. Ces éléments, mis à jour si nécessaire lors de la contractualisation, sont annexés au contrat signé avec les tiers. Des dispositions particulières définissent les points à prendre en compte lors de la clôture du contrat afin de garantir la sécurité du SI de l'établissement postérieurement à celui-ci. C'est en particulier le cas pour les clauses de réversibilité.

[ISO 27001 - A 10.2.1]	Prestation de service

[TIERS_04] Prestation de services par un tiers

Les obligations en matière de sécurité relatives aux services fournis par des tiers et au niveau de prestation attendu sont formalisées, généralement dans le cahier des charges de la prestation.

Ces obligations sont mises en œuvre, appliquées et tenues à jour conformément à ce qui est défini par les accords contractuels.

[ISO 27001 - A 10.2.2]	Surveillance et examen des services tiers

[TIERS_05] Surveillance et examen des services tiers

Les services fournis par des tiers sont si nécessaire contrôlés et évalués .L'existence et les modalités de cet examen périodique sont précisées dans les contrats ou conventions conclues avec les tiers.

[ISO 27001 - A 10.2.3]	Gestion des modifications dans les services tiers

[TIERS_06] Gestion des modifications dans les services tiers

L'évolution du Système d'Information, des besoins de sécurité ou l'identification de nouveaux risques peuvent notamment apporter des changements au niveau des services tiers.

7. Sécurité physique et environnementale

7.1. Structuration de l'infrastructure en zones de confiance

[ISO 27001 - A 9.1.1]	Périmètre de sécurité physique
[ISO 27001 - A 9.1.2]	Contrôle physique des accès

[PHY_01] Définition des périmètres de sécurité physique

Afin d'empêcher tout accès physique non autorisé, tout dommage ou intrusion dans les locaux et informations, des périmètres de sécurité sont définis. La définition des zones est adaptée au contexte d'utilisation des locaux de l'Établissement et à leur accès par les différentes catégories de personnes.

- Les zones publiques permettant l'accès aux ressources de l'établissement.
- Les zones sensibles donnant accès aux bureaux de personnes à responsabilité ou titulaires de postes de confiance ainsi qu'aux plateformes de développement doivent être fermées physiquement en l'absence des personnes.
- Les zones machines dédiées aux équipements informatiques (serveurs, calculateurs) et au réseau. Il s'agit de bâtiments ou de locaux dédiés, protégés par un contrôle d'accès spécifique.
- Quelle que soit la zone, un poste d'utilisateur doit toujours être sécurisé en l'absence même temporaire de l'usager, soit en fermant à clé la porte du bureau soit, au moins, en verrouillant la session.

[ISO 27001 - A 9.2.1]	Choix de l'emplacement et protection du matériel

[PHY_02] Protection physique et environnementale des matériels

La localisation des équipements dans les zones est adaptée à la sensibilité des informations qu'ils supportent et au besoin de disponibilité du service qu'ils fournissent.

7.2. Contrôle des accès physiques, gestion des autorisations

[ISO 27001 - A 9.1.2]	Contrôle physique des accès
[ISO 27001 - A 9.1.3]	Sécurisation des bureaux, des salles et des équipements

[PHY_03] Mise en œuvre des contrôles des accès physiques

Des moyens de protection contre les accès physiques sont définis et mis en œuvre pour chacune des zones sensibles et des machines.

[PHY_04] Gestion des autorisations des accès physiques

Sauf situation très spécifique encadrée par une procédure formalisée, les zones machines ne doivent être accessibles qu'en présence d'un personnel chargé de la maintenance informatique.

[PHY_05] Contrôle et suivi des autorisations des accès physiques

Tout responsable de locaux sensibles maintient sous sa responsabilité une liste des personnes disposant d'autorisations d'accès à ces locaux. Cette liste est revue à chaque mouvement de personnel.

7.3. Accueil et accompagnement des visiteurs

[ISO 27001 - A 9.1.2]	Contrôle physique des accès

[PHY_06] Accueil des visiteurs

Les zones publiques sont en circulation libre pour les visiteurs. Dans les autres zones les visiteurs doivent être accompagnés.

[ISO 27001 - A 9.1.6]	Zones d'accès public, de livraison et de chargement

[PHY_07] Zones d'accès publiques, de livraison et de chargement

Les zones de livraison et de chargement sont situées dans des zones publiques.

.

7.4. Mise au rebut sécurisée

[ISO 27001 - A 9.2.6]	Mise au rebut ou recyclage sécurisé(e) du matériel

[PHY_08] Destruction des biens sensibles

Les procédures de mise au rebut des biens sensibles sont formalisées et communiquées à l'ensemble du personnel présentant un besoin d'en connaître

La mise au rebut des supports papiers contenant des informations sensibles est réalisée au moyen d'une déchiqueteuse ou d'un incinérateur. La conservation des documents est effectuée en lieu sûr avant leur destruction.

La mise au rebut des supports électroniques (exemple disques durs) est OBLIGATOIREMENT réalisée de manière sécurisée : par effacement (à minima un formatage)puis par neutralisation physique (broyage, poinçonnage) conformément aux préconisations de l'établissement. . La conservation des matériels est effectuée en lieu sûr avant destruction.

7.5. Protection contre les menaces extérieures et environnementales

[ISO 27001 - A 9.2.1]	Choix de l'emplacement et protection du matériel

[PHY_09] Localisation des matériels

Les matériels du système d'information, présentant une valeur attractive, fragiles, ou supports d'information sensibles sont disposés dans des emplacements appropriés garantissant leur sécurité (imprimantes, vidéoprojecteurs, ordinateurs en libre-service, serveurs de données, etc…).

Notamment ces matériels sont entreposés dans des salles ou armoires fermées à clés en l'absence des personnes responsables. Ils disposent par ailleurs d'équipements contre le vol, de marquages indélébiles pour empêcher la revente, ou toutes autres mesures jugées utiles.

7.6. Surveillance et protection du site

[ISO 27001 - A 9.1.2]	Contrôle physique des accès
[ISO 27001 - A 9.1.3]	Sécurisation des bureaux, des salles et des équipements

[PHY_10] Gestion des données de vidéosurveillance

La rétention des données de vidéosurveillance est effectuée sur une fenêtre d'une durée en conformité avec les préconisations de la CNIL. Les vidéos de surveillance sont conservées sur un dispositif dédié et sécurisé. dont la console d'exploitation est restreinte aux seules personnes habilitées.

[PHY_11] Surveillance des locaux informatiques

Des rondes sont régulièrement effectuées au minimum sur les zones sensibles ou les zones serveurs. Un cahier de passage devra être mis en place.

7.7. Équipement d'infrastructure du site

[ISO 27001 - A 9.2.2]	Services généraux
[ISO 27001 - A 9.1.4]	Protection contre les menaces extérieures et environnementales

[INFRA_01] Adéquation des équipements d'infrastructure

Toute structure retenue par la DSI pour héberger des ressources serveurs dispose des équipements d'infrastructure nécessaires à leur bon fonctionnement et à leur sécurité : climatisation, alimentation électrique secourue. Une attention particulière sera portée à leur bon dimensionnement.

[INFRA_02] Redondance des équipements d'infrastructure

Les équipements d'infrastructure du site présentent un niveau de redondance suffisant pour assurer un bon fonctionnement de l'infrastructure et des moyens informatiques, compatible avec le Plan de Continuité d'Activité établi pour le site.

[ISO 27001 - A 9.2.4]	Maintenance du matériel

[INFRA_03] Maintenance des équipements d'infrastructure

Les équipements d'infrastructure sont couverts par des contrats de maintenance (ou des pièces de rechange stockées) et si nécessaire par des contrats de services permettant d'assurer la disponibilité du service rendu par ces équipements. Ces dispositions sont à la charge des structures qui en font l'acquisition. pour la durée de vie prévisible du matériel.

[ISO 27001 - A 9.2.3]	Sécurité du câblage

[INFRA_04] Protection des câbles

Les salles informatiques comportent des dispositifs appropriés permettant un passage sécurisé des différents câblages.

Un plan de câblage à jour est formalisé et est rendus accessible au personne dont le travail en nécessite la connaissance et en particulier à ceux participant au PCA.

Dans chaque site participant au PCA les câbles doivent être étiquetés à chaque extrémité ainsi que les ports utiles des appareils actifs.

8. Habilitation et contrôle d'accès logique

8.1. Gestion des habilitations

[ISO 27001 - A 11.2.1]	Enregistrement des utilisateurs

[HGDA_01] Gestion des profils et des droits alloués

Une matrice des droits doit être établie sur chaque SI métier en bannissant les comptes génériques.

Une procédure de gestion des habilitations définit les principes de gestion des profils et des droits correspondants en termes d'accès aux ressources du Système d'Information (en particulier les outils de gestion hébergés à la DSI Centrale, bâtiment du CRRI). La gestion des habilitations concerne les chercheurs, enseignants, étudiants, agents administratifs par métier.

Cette procédure couvre la création, la modification et la suppression des comptes de l'utilisateur, et donc des droits associés à ces profils.

Les droits alloués à chaque profil sont limités aux seuls droits nécessaires à l'accomplissement des missions qui incombent aux titulaires de ce profil.

La liste des profils et des droits alloués à chaque profil est tenue à jour. Les profils comme les droits alloués sont périodiquement révisés par la DSI et le responsable hiérarchique de l'utilisateur.

[ISO 27001 - A 11.2.2]	Gestion des privilèges

[HGDA_02] Demandes concernant les habilitations et droits d'accès

Un document précise les habilitations et droits d'accès par défaut aux applications et aux serveurs, selon les catégories de profils.

Pour tous les profils la demande et l'allocation de droits d'accès se réalisent suivant une procédure identifiée.

Pour les profils de type étudiants ou usagers, l'allocation des droits d'accès à un bouquet de services est systématique (accès à des ressources autorisées de base telles que des ressources documentaires, les portails d'information de l'établissement, l'accès Internet,…).

Pour tous les autres types de profil (tiers et prestataires ponctuels par exemple), les habilitations sont effectuées au cas par cas; une date de retrait des droits est systématiquement définie et la suppression des droits est contrôlée.

L'historique des demandes d'habilitations et de droits d'accès est conservé.

[HGDA_03] Validation des demandes concernant les habilitations et droits d'accès

Il convient que le responsable DSI métier de l'application ou des données pour lesquelles des droits sont demandés valide chaque demande préalablement à l'ouverture des droits, après consultation du responsable fonctionnel (ou sur sa demande).

Un processus de demande est défini et adapté à chaque profil, pour la validation d'accès aux ressources demandées.

L'historique de ces validations de demandes doit être conservé par la direction métier responsable.

[ISO 27001 - A 11.2.4]	Réexamen des droits d'accès d'utilisateur

[HGDA_04] Suivi et révision des habilitations et droits d'accès

Des revues formalisées des profils et des droits d'accès associés ainsi que des habilitations (utilisateurs auxquels les profils sont attribués) ont lieu tous les ans. Ces revues visent à supprimer les éventuels accès inappropriés. Ces revues sont menées par les responsables d'application. Elles s'appuient sur les règles de l'Etablissement en matière d'autorisations informatiques formalisées par des matrices de droits d'accès.

.

[HGDA_05] Retrait des habilitations et droits d'accès

Un processus de retrait des droits d'accès est défini selon les profils (en particulier révisé pour les agents à chaque changement de poste ou de fonction)

Les droits d'accès des étudiants sont systématiquement supprimés en conformité avec le calendrier défini dans la politique de gestion des comptes.

8.2. Droits d'accès

[ISO 27001 - A 11.4.1]	Politique relative à l'utilisation des services en réseau
[ISO 27001 - A 11.5.2]	Identification et authentification de l'utilisateur

[CA_01] Identification et authentification

Les utilisateurs du SI sont identifiés individuellement, de manière unique et normalisée. A chaque identifiant est associé un authentifiant respectant les exigences stipulées en la matière. Des identifiants supplémentaires peuvent être utilisés dans les composantes de l'UCA en fonction des contraintes locales. Ces éventuelles dérogations ne doivent pas remettre en question l'obligation d'identification personnelle et doivent être conformes à celle de l'UCA en termes d'exigence de sécurité.

[ISO 27001 - A 11.2.3]	Gestion du mot de passe utilisateur

[CA_02] Gestion des comptes

Une procédure formelle décrit la manière dont les comptes utilisateurs sont gérés, et en particulier comment ils sont créés, modifiés ou supprimés, selon les applications et les profils. Les règles de diffusion des identifiants aux utilisateurs sont aussi formalisées.

[CA_03] Caractéristiques des comptes

Tout compte permet d'identifier son titulaire.

Les identifiants respectent la codification interne de l'établissement.

[ISO 27001 - A 11.3.1]	Utilisation du mot de passe

[CA_04] Caractéristiques des authentifiants

Des documents d'application définissent les principes de gestion des authentifiants.

Lorsque des mots de passe sont utilisés comme authentifiants, ils respectent les règles de bonnes pratiques spécifiées dans la note de sécurité relative à l'usage des mots de passe.

Des dérogations à ces règles sont limitées aux applications qui ne supportent pas ces contraintes.

[CA_05] Confidentialité des authentifiants

Des mesures garantissent la confidentialité des authentifiants circulant sur le réseau (utilisation de protocoles sécurisés, réseau d'administration isolé).

Les utilisateurs doivent protéger leurs mots de passe et ne les communiquer à personne.

[ISO 27001 - A 11.5.3]	Système de gestion des mots de passe

[CA_06] Systèmes de gestion des mots de passe

Les logiciels ou fonctions utilisés pour générer ou contrôler les mots de passe choisis par l'utilisateur répondent aux exigences basiques de sécurité, en refusant les mots de passe qui ne répondent pas aux critères retenus à la section CA_04.

Les mots de passe sont stockés de façon chiffrée et sécurisée par la mise en œuvre de méthodes reconnues.

[ISO 27001 - A 11.4.3]	Identification des matériels en réseau

[CA_07] Identification des matériels en réseau

Les matériels sont automatiquement identifiés lors de leur raccordement sur le réseau, et seuls les matériels autorisés peuvent se connecter aux réseaux internes qualifiés de sensibles (réseau applicatif). Au minimum, le contrôle est réalisé obligatoirement par authentifiant pour les réseaux Wifi, par adresse IP ou adresse Mac pour les réseaux filaires. Le contrôle d'accès au VPN se fait au minimum par vérification des authentifiants.

8.3. Suivi des accès

[ISO 27001 - A 10.10.2]	Surveillance de l'exploitation du système

[CA_08] Suivi des accès

Tous les accès aux données sensibles et fonctions sensibles sont tracés et sont régulièrement analysés et contrôlés.

Les traces sont sauvegardées et conservées de façon sécurisée pendant une période de temps suffisante pour répondre aux besoins opérationnels et satisfaire les exigences réglementaires.

[ISO 27001 - A 8.3.3]	Retrait des droits d'accès

[CA_09] Traitement des comptes inactifs

La politique de gestion des comptes fixe les délais de désactivation, d'archivage et de suppression des comptes non initialisés ou plus utilisés.

8.4. Gestion des comptes privilégiés

[ISO 27001 - A 11.2.2]	Gestion des privilèges

[CPRIV_01] Gestion des comptes privilégiés

Les comptes privilégiés et les droits alloués à ces comptes sont gérés au même titre que tout autre compte par les responsables de structure ou d'application.

Ils sont réservés aux administrateurs et aux exploitants. Une liste des administrateurs et exploitants ayant accès aux comptes privilégiés, est établie et maintenue à jour. Pour tout compte privilégié partagé, cette liste indique le responsable identifié et la liste des personnes ayant accès à ce compte.

Cette liste, dont le contenu est considéré comme sensible, est à usage exclusif de la structure ou du RSSI en cas de demande.

[CPRIV_02] Gestion des comptes systèmes génériques ou partagés

Ils sont à considérer et à traiter comme des comptes privilégiés [CPRIV_O1] . Rentrent dans cette catégorie les comptes tels que « root » sous Unix ou « administrateur/administrator » sous Windows, les comptes dédiés à l'administration de progiciels, les comptes d'équipement réseau actif, …

L'utilisation des comptes privilégiés partagés est limitée au strict nécessaire. L'utilisation de comptes systèmes nominatifs doit être la règle.

Si un compte système est utilisé par une autre personne que le titulaire ou un utilisateur accrédité, l'utilisation se fait en présence du titulaire du compte ou d'une personne qualifiée pour le représenter.

[CPRIV_03] Gestion des comptes systèmes personnels

Les comptes systèmes personnels sont des comptes privilégiés nominatifs avec des privilèges / droits équivalents aux comptes systèmes qu'ils remplacent.

Des comptes systèmes nominatifs sont créés pour chaque personne justifiant de l'utilisation d'un compte privilégié. Ils diffèrent des comptes « bureautiques » ou « applicatifs » de leurs titulaires.

[CPRIV_04] Gestion des comptes systèmes utilisés par les constructeurs

Il s'agit principalement de comptes destinés à l'installation ou à la maintenance des matériels et des logiciels.

Les comptes destinés uniquement à l'installation des produits sont rendus inopérants dès l'installation terminée.

Les comptes destinés uniquement à la maintenance sont désactivés en dehors des opérations de maintenance.

[CPRIV_05] Authentification des comptes à privilèges élevés

Les mots de passe sont conformes à la politique de gestion des authentifiants , en particulier

- modifiés avec une fréquence définie.
- changés après toute utilisation temporaire du compte par un tiers (ex : compte de production utilisé ponctuellement par un développeur).
- changés dès qu'une personne sort de la liste des utilisateurs autorisés.

[CPRIV_06] Disponibilité des comptes à privilèges élevés

Des mesures permettent d'assurer la disponibilité des mots de passe des comptes privilégiés pour un usage urgent par un autre administrateur de l'établissement.

[ISO 27001 - A 11.5.4]	Emploi des utilitaires systèmes

[CPRIV_07] Restriction d'emploi des utilitaires systèmes et de sécurité

L'utilisation des programmes permettant de contourner les mesures de sécurité, notamment en accédant directement à l'information stockée ou transportée, sans passer par la couche applicative, est fortement encadrée et tracée, et réservée aux administrateurs autorisés. Il en va de même pour l'utilisation de tout utilitaire de sécurité, permettant par exemple de connaître ou de manipuler le paramétrage des systèmes, d'accéder aux fichiers de journalisation, ou de réaliser toute autre action dangereuse.

L'installation et l'utilisation de tels outils par des utilisateurs non administrateurs sont proscrites.

8.5. Séparation des rôles

[ISO 27001 - A 10.1.3]	Séparation des tâches

[HGDA_06] Séparation des tâches

Afin de limiter les risques d'erreur ou de mauvais usages, il convient d'établir une séparation des tâches et des responsabilités entre :

- les personnes chargées d'autoriser les droits d'accès applicatifs.
- les personnes utilisant les comptes applicatifs.
- les personnes chargées d'attribuer les droits.

[ISO 27001 - A 10.1.4]	Séparation des équipements de développement, de test et d'exploitation

[HGDA_07] Séparation des environnements

Les différents environnements et équipements (développement, test, exploitation…) sont séparés.

Les règles de passage d'un environnement à l'autre sont formalisées et documentées.

9. Sécurité des réseaux

9.1. Architecture des réseaux

[ISO 27001 - A 10.8.5]	Systèmes d'information d'entreprise

[NET_01] Passerelles Internet et de sécurité

Des équipements d'infrastructure sont mis en place afin de protéger et d'isoler les réseaux internes vis-à-vis de l'extérieur au niveau du pôle infrastructure de la DSI (RENATER)

Le modèle d'architecture réseau préconisé par l'Université est celui d'une boucle sécurisée de distribution, centralisée, redondante et gérée par l'équipe réseau du pôle infrastructures de la DSI, sur laquelle viennent se connecter les équipements de routage et de sécurisation (par exemple un pare-feu) de chaque structure, ainsi que les points de raccordement aux ressources mutualisées (ENT, applications AMUE) et ressources extérieures (RENATER, CRATERE, …). L'objectif est d'avoir une architecture résiliente, modulaire, structurée et cloisonnée.

.

[NET_02] Plan d'adressage

L'utilisation d'adresses IP non routables et d'un mécanisme de traduction d'adresses est la règle par défaut. Les adresses routables sont gérées pour assurer la rationalisation de leur utilisation et leur bon référencement (titulaire, matériel, localisation, usage) Les adresses des postes clients sont affectées via un système DHCP (sauf cas exceptionnel) afin de les recenser efficacement, de pouvoir les bloquer rapidement en cas de problème et d'interdire l'utilisation de matériels personnels non normés.

[NET_03] Cloisonnement des réseaux

Aucun équipement de l'Établissement ne peut être connecté directement au Réseau Internet. Toute connexion transite par une DMZ. Toute exception fait l'objet d'une demande de dérogation.

Des zones ou périmètres de sécurité sont définis afin de cloisonner le Système d'Information en différents périmètres de niveaux de confiance homogènes:

- Réseau Internet : zones directement connectées à Internet, non maîtrisées et disposant d'un niveau de confiance nul.
- LAN Internet : zones de confiance basse, ouvertes sur le réseau Internet au travers d'une DMZ (le réseau interne de l'Université).

- LAN interne : zones maîtrisées disposant d'un bon niveau de confiance. Elles hébergent l'ensemble des ressources du Système d'Information. Ces zones n'ont pas de connexion directe avec le réseau Internet.
- DMZ : zones maîtrisées mais disposant d'un niveau de confiance modéré. Elles hébergent les équipements assurant l'interface entre les LAN internes d'une part, le réseau Internet d'autre part, et garantissent la protection des premiers vis-à-vis des seconds.

[NET_04] Partitionnement des réseaux

Autant que possible le LAN interne est partitionné en sous-réseaux afin d'assurer un isolement des « branches sensibles » et de permettre de confiner, si besoin est, une branche réseau en cas d'incident.

Les connexions sont filtrées et un contrôle d'accès activé au niveau d'un sous-réseau.

Le cloisonnement à minima est réalisé pour séparer les périmètres suivants :

- Les serveurs dans un réseau avec des protections adaptées
- Les postes des personnels et assimilés
- Les postes à destination des étudiants
- Les connexions dites de nomadisme
- Les connexions destinées aux postes des invités

[ISO 27001 - A 11.6.2] Isolement des systèmes sensibles

[NET_05] Isolement des réseaux sensibles

Sont considérés comme réseaux sensibles :

- les réseaux hébergeant des serveurs ou applications contenant des informations sensibles ou des processus métiers sensibles, tels que les serveurs d'applications en production, les serveurs de sécurité (annuaire, firewall, proxy, serveur d'authentification), les serveurs de sauvegarde, les réseaux des laboratoires.
- les réseaux pour lesquels la sécurité n'est pas connue ou pas maîtrisée par l'établissement (réseaux d'un partenaire, d'un laboratoire, réseau invité).

Il convient de cloisonner les réseaux sensibles vis-à-vis du LAN interne par des mesures de sécurité réseau (pare-feu, antivirus, proxy, VLAN, authentification…).

Tout accès depuis un réseau extérieur sur une machine connectée à un réseau de l'Établissement est soumis à autorisation et validé de manière formelle en conformité avec la politique d'accès de l'Établissement.

9.2. Documentation des réseaux

[ISO 27001 - A 10.1.1] Procédures d'exploitation documentées

[NET_06] Identification de l'infrastructure réseau

L'infrastructure réseau est répertoriée et documentée. Une description de cette infrastructure est tenue à jour en incluant :

- Une cartographie du réseau recensant les principaux éléments de l'infrastructure et présentant l'organisation générale du réseau (lignes spécialisées, LAN, accès Internet, autres accès…)

- Un recensement des principaux flux de données internes ou externes,
- Un descriptif détaillé du câblage interne,
- Un inventaire des équipements, leur localisation et leur configuration,

[NET_07] Documentation d'administration et d'exploitation des réseaux

Les procédures d'exploitation du réseau sont formalisées et documentées. Parmi ces procédures, une attention toute particulière est apportée à la procédure d'ouverture de règles au niveau des équipements de filtrage réseau.

L''infrastructure réseau et sa configuration sont documentées.

La documentation est tenue à jour. L'accès à cette documentation est limitée aux seules personnes ayant besoin de la connaître.

La documentation réseau est actualisée lors de toute modification fonctionnelle des flux ou de l'infrastructure technique. Elle est revue au minimum une fois par an.

[ISO 27001 - A 10.7.4]	Sécurité de la documentation système

[NET_08] Protection de la documentation et des données réseau

La documentation réseau et les procédures d'administration et d'exploitation des réseaux sont des documents sensibles. Elles sont protégées contre tout accès non autorisé par des personnes ne disposant pas du besoin d'en connaître. Dans tous les cas, la sécurité du Système d'Information ne doit pas reposer uniquement sur ce simple secret.

9.3. Administration et exploitation des réseaux

[ISO 27001 - A 10.6.1]	Mesures sur les réseaux

[NET_09] Journaux des opérations d'administration et d'exploitation des réseaux

Les opérations sensibles d'administration sont tracées et journalisées, au moyen de rapports d'intervention pour les opérations physiques, via l'enregistrement des connexions pour les opérations logiques.

Les journaux sont sauvegardés et conservés pendant une période adaptée aux besoins de suivi et contrôle, en respectant les exigences réglementaires.

[NET_10] Dimensionnement des réseaux

Il convient de surveiller les activités réseaux et de s'assurer que l'infrastructure réponde aux besoins de disponibilité, de dimensionnement et de qualité de service de l'Établissement.

[NET_11] Contrôle d'accès logique aux équipements réseau

Un contrôle d'accès logique aux équipements réseaux est mis en œuvre.

Les mots de passe « constructeur » paramétrés par défaut sur les équipements sont systématiquement modifiés. Si possible, des comptes d'administration et de supervision nominatifs sont créés. Les mots de passe en sont régulièrement modifiés.

Dans la mesure du possible, il est régulièrement procédé à un contrôle des accès aux équipements réseaux et des droits alloués aux administrateurs et aux exploitants.

[ISO 27001 - A 11.4.4]	Protection des ports de diagnostic et de configuration à distance

[NET_12] Protection de l'administration réseau

L'administration et la supervision des réseaux sont effectuées depuis des réseaux et des équipements dédiés.

L'accès aux ports (physiques et logiques) d'administration et de supervision est contrôlé et limité aux équipements ou réseaux dédiés.

[NET_13] Surveillance continue de l'activité sur les réseaux

Le responsable informatique assure une surveillance continue des réseaux sous sa responsabilité.

Cette surveillance porte notamment sur :

- Le contrôle du bon fonctionnement des réseaux.
- Le contrôle de la charge des réseaux et de leur disponibilité.
- L'utilisation réalisée au travers des réseaux.

Cette surveillance s'appuie sur des moyens dédiés et protégés, qui sont éventuellement partagés avec ceux utilisés pour l'administration et l'exploitation des systèmes et des réseaux.

[ISO 27001 - A 10.10.4]	Journal administrateur et journal des opérations

[NET_14] Journalisation des événements réseau

Des dispositifs d'audit sont mis en place qui permettent l'enregistrement dans des fichiers de traces (dits journaux d'audit) des principaux événements liés à la sécurité des réseaux.

Cette journalisation porte notamment sur les événements suivants :

- Les anomalies pouvant être révélatrices d'un incident de sécurité.
- Les atteintes à la sécurité : détections de virus, tentatives d'intrusion, erreurs de connexion…
- L'activité des personnes en charge de l'exploitation des réseaux : configuration et paramétrage des équipements de communication, gestion des habilitations et des droits d'accès…
- Les événements liés à l'accès au réseau, à la volumétrie des échanges, aux connexions des nomades…

Les journaux d'audit sont systématiquement revus afin de détecter les problèmes de sécurité.

[NET_15] Conservation des journaux réseau

Les journaux d'audit sont des biens sensibles, qui sont sauvegardés et protégés. Ils sont conservés pendant une période suffisante pour répondre aux besoins opérationnels tout en satisfaisant les exigences légales, réglementaires ou contractuelles. Cette gestion se fait en conformité avec la politique de gestion des journaux informatiques.

9.4. Sécurité de l'infrastructure réseau

Par infrastructure réseau, on entend les équipements matériels et logiciels, le câblage, les prises réseaux.

[ISO 27001 - A 10.6.2]	Sécurité des services réseau

[NET_16] Sécurisation des équipements d'infrastructure réseau

Les configurations des équipements d'infrastructure réseau bénéficient de mesures de durcissement.

Elles concernent à minima les aspects :

- Sécurisation de l'accès, contrôle d'accès logique à l'interface d'administration
- Désactivation des ports et services non utilisés (telnet, rlogin, ftp, etc…)
- Sélection des composants logiciels, désactivation des utilitaires et paquetages non utilisés
- Gestion des comptes et privilèges d'administration
- Mises à jour des correctifs de sécurité
- Activation des traces d'audit
- Stratégie de sécurité (mot de passe, verrouillage)

[ISO 27001 - A 9.2.3]	Sécurité du câblage

[NET_17] Protection du câblage et des prises réseau

Les prises réseau sont identifiées et localisées, et **seuls les ports nécessaires sont activés** . L'accès aux panneaux de raccordement et aux tableaux de brassage est sécurisé. L'accès aux têtes de ligne est contrôlé et protégé. Les opérateurs sont sensibilisés aux risques d'interception ou de dégradations sur le câblage.

[ISO 27001 - 10.6.1]	Mesures sur les réseaux

[NET_18] Disponibilité des équipements réseau

Les équipements d'infrastructure critiques (tels que les routeurs, les commutateurs fédérateurs) sont redondés dès que possible ; à défaut, des matériels de remplacement sont disponibles.

9.5. Équipements non maîtrisés par l'établissement

Par équipements non maîtrisés par l'établissement, on entend les équipements réseau (modems, routeurs, etc.) voire de sécurité (ces équipements peuvent contenir des fonctions de sécurité) mis en œuvre ou administrés par des tiers (Ces tiers sont généralement des opérateurs de télécommunication). Ces équipements peuvent être la propriété de l'établissement ou de ces tiers. Leur installation peut être faite sous la responsabilité de l'établissement ou de ces tiers.

[ISO 27001 - A 7.1.1]	Inventaire des biens

[NET_19] Identification des équipements non maîtrisés

Il convient d'identifier et de répertorier les équipements réseau et de sécurité non maîtrisés par l'établissement.

[ISO 27001 - A 6.2.1]	Identification des risques provenant des tiers

[NET_20] Sécurité des équipements non maîtrisés

En l'absence d'un contrat spécifique prenant en compte la sécurité, il convient de considérer comme inexistantes les fonctions de sécurité disponibles sur les équipements non maîtrisés par l'établissement.

Les mesures de sécurité ne doivent pas reposer sur celles proposées par les équipements non maîtrisés, tels que fournis par les services des Fournisseurs d'Accès Internet (sauf contractualisation spécifique).

10. Sécurité des échanges de données

10.1. Dispositions générales sur les flux réseaux

[ISO 27001 - A 11.4.6]	Mesures relatives à la connexion réseau

[NET_21] Contrôle des accès réseau

Tout flux de communication (flux et protocoles réseau) sur le SI de l'Etablissement, entrant ou sortant, est soumis à autorisation préalable. La demande est formalisée, validée par le responsable hiérarchique et soumise à accord de la DSI et du RSSI.

L'accès à Internet est individualisé et authentifié et donne lieu à journalisation des accès dans la limite des textes en vigueur.

Un mécanisme d'authentification renforcée est utilisé pour les accès entrants depuis un Réseau Internet vers le LAN internet.

Un registre des autorisations est tenu à jour pour les accès entrants. Toute demande devra être justifiée. L'autorisation est donnée le cas échéant pour une durée maximum d'une année.

[ISO 27001 - A 10.6.2]	Sécurité des services réseau

[NET_22] Protection des flux réseau

Toute interconnexion entre les réseaux de l'Établissement et l'extérieur est validée par la DSI et le RSSI. Tout échange respecte le principe du moindre privilège.

[NET_23] Analyse des flux réseau

Tous les flux réseaux sont analysés par un mécanisme de contrôle (tel qu'un antivirus ou par d'autres mécanismes tels qu'un système proxy, un dispositif de détection d'intrusion, etc.)

Les flux jugés dangereux (mails, attaques, etc.) sont bloqués.

[NET_24] Traçabilité, surveillance et alerte

Des équipements sont mis en œuvre pour assurer la traçabilité des accès et des flux entrants et sortants avec le réseau Internet, et pour l'accès aux applications métiers sensibles.

Les événements tracés sont enregistrés et les traces protégées du point de vue disponibilité, intégrité et confidentialité.

Les équipes réseau effectuent un monitoring des événements critiques (alarmes) remontés par les équipements ainsi qu'une analyse quotidienne des journaux d'événements. Les alarmes et les événements susceptibles de révéler un incident de sécurité sont investigués. L'alerte est donnée au RSSI dès qu'un incident de sécurité est suspecté. Des mesures conservatoires peuvent être prises en attente de l'avis du RSSI.

10.2. Accès à l'Internet depuis le réseau interne de l'Établissement

Ces accès sont caractérisés par le fait que les sites et services accédés ont un niveau de confiance inconnu.

[ISO 27001 - A 11.4.1]	Politique relative à l'utilisation des services en réseau

[INET_01] Autorisation d'accès à Internet

L'accès au réseau Internet (web) est systématiquement autorisé dans la limite de la charte RENATER et de la politique de l'établissement. Il peut être retiré sur demande de la hiérarchie ou de la DSI en cas de violation des règles d'usage du service.

L'accès alloué est personnel. Il est réservé à un usage professionnel ou pédagogique. Les utilisations de cet accès sont tracées et journalisées et font l'objet d'un examen périodique.

[INET_02] Diffusion des règles d'accès et d'utilisation

Les règles régissant la navigation sur Internet et l'utilisation des outils de communication sont formalisées dans une charte utilisateur, diffusées à l'ensemble du personnel, connues et acceptées.

[ISO 27001 - A 10.4.1]	Mesures contre les codes malveillants

[INET_03] Analyse des fichiers entrants et sortants

Dans la mesure du possible, tout contenu transmis ou récupéré par un utilisateur fait l'objet d'une analyse protégeant des logiciels malveillants. Cela s'applique outre les fichiers transmis par mail, à tous les fichiers téléchargés.

[INET_04] Contrôle des accès et de l'utilisation

Des mesures de contrôle d'accès et d'utilisation de l'Internet sont mises en œuvre :

- Dès que possible, les contenus des flux sont analysés à la recherche de codes malveillants
- Toutes les connexions sont tracées, journalisées et analysées conformément à la politique de gestion des journaux informatiques

10.3. Accès aux sites Web de l'Établissement depuis l'Internet

Ces accès sont caractérisés par le fait que le tiers accédant n'est pas, a priori, « de confiance ». Ce peut être par exemple une structure partenaire, un étudiant et tous les accès volontairement malveillants.

Ces sites et services Web permettent :

- *La publication d'informations destinées à tous*
- *Le recueil d'informations issues des tiers identifiées ou non identifiés*

[ISO 27001 - A 10.9.3]	Informations à disposition du public

[INET_05] Publication de données sur Internet

Les informations institutionnelles destinées à être publiées sont validées préalablement à leur mise en ligne en conformité avec la hiérarchie de l'établissement. L'authenticité des informations mises en ligne est régulièrement contrôlée par leur propriétaire.

[ISO 27001 - A 15.1.4]	Protection des données et confidentialité des informations relatives à la vie privée

[INET_06] Recueil d'informations personnelles auprès de tiers (connus ou inconnus)

Ces informations (demandes, coordonnées…) sont collectées par l'Établissement dans un but précis et peuvent être confidentielles ou à caractère personnel.

À ce titre :

- Les informations collectées font l'objet d'une déclaration auprès du Correspondant Informatique et Libertés (CIL) ou du Délégué de la Protection des Données (DPD) et sont protégées contre tout accès non autorisé.
- La personne doit être explicitement informée de la finalité du recueil ainsi que de son droit de consultation et de rectification ou de suppression des données personnelles recueillies.

[ISO 27001 - A 12.2.1]	Validation des données d'entrée
[ISO 27001 - A 10.4.1]	Mesures contre les codes malveillants
[ISO 27001 - A 10.4.2]	Mesures contre le code mobile

[INET_07] Contrôle des informations mises à disposition

Les informations reçues et mises à disposition par l'Établissement, sont analysées (recherche de virus et de codes mobiles, détection de signatures d'attaque…) et filtrées afin d'éliminer tout élément malveillant, et d'éviter sa retransmission.

10.4. Accès pour les partenaires et accès à des services tiers externes

Ces échanges sont établis avec des partenaires connus et identifiés et répondent à des besoins « formalisables ».

Ils permettent :

- *La mise à disposition avec ces partenaires d'informations à diffusion limitée*
- *L'utilisation, depuis l'Internet ou le LAN Interne, d'applicatifs permettant de gérer des données qualifiées*
- *Des échanges spécifiques, (tel que la transmission d'ordres de virement). Ces échanges s'appuient souvent sur des protocoles spécialisés et des outils dédiés.*

[ISO 27001 - A 6.2.1]	Identification des risques provenant des tiers

[EDI_01] Formalisation des services et des échanges applicatifs

Les services et les échanges applicatifs mis à la disposition de tiers comme l'utilisation de services tiers externes sont définis dans le cadre de projets qui incluent une analyse sécurité permettant :

- D'identifier les connexions et flux de données nécessaires sur un plan fonctionnel ou technique.
- De déterminer leurs besoins de sécurité (confidentialité, intégrité, authenticité, non-répudiation).
- D'évaluer la menace et les risques induits.
- De sélectionner des contre-mesures permettant de ramener ces risques à un niveau acceptable.

[EDI_02] Autorisation d'accès

L'ouverture d'un accès pour un tiers est soumise à autorisation et nécessite, éventuellement, la signature d'un accord préalable entre ce tiers et l'Établissement. Il en est de même pour tout accès à un service tiers externe. Ces accords contractuels incluent l'aspect sécurité et définissent les procédures à respecter.

[EDI_03] Contrôle des accès et protection des échanges

Le tiers – système, applicatif ou utilisateur – accédant au système d'information de l'établissement, est identifié et authentifié. L'utilisation d'un protocole sécurisé (SSL, SSH) ou d'une liaison garantissant cette identité (VPN) est recommandée.

Les connexions établies et les échanges réalisés sont tracés, journalisés et audités.

10.5. Utilisation du Wifi

[ISO 27001 - A 10.6.1]	Mesures sur les réseaux

[WIFI_01] Utilisation du Wifi dans l'établissement

L'accès aux points de connexion WiFi est contrôlé, et réservé aux seuls utilisateurs autorisés.

Des mesures d'authentification des utilisateurs accédant aux points d'accès Wifi, et des mesures de chiffrement des flux Wifi sont réalisées en fonction du besoin.

Les seuls réseaux autorisés sont ceux validés par la DSI et le RSSI et transitant par les points d'accès de l'Université.

Le seul référentiel d'utilisateurs autorisé est l'annuaire de l'établissement.

11. Sécurité des serveurs et des systèmes

Par systèmes et serveurs, on entend les serveurs bureautiques, les serveurs applicatifs et les serveurs dits d'infrastructure (serveurs hébergeant des services transversaux nécessaires au fonctionnement du SI : serveurs de messagerie, serveurs de domaine Active Directory), ainsi que les systèmes dits de sécurité tels que des pare-feu, serveurs antivirus, proxies,…

11.1. Configuration et gestion des configurations

[ISO 27001 - A 10.1.1]	Procédures d'exploitation documentées

[EXP_01] Sécurisation des serveurs

Les systèmes d'exploitation des serveurs bénéficient de mesures de durcissement.

Elles concernent à minima les aspects :

- Contrôle d'accès physique au système
- Désactivation des ports et services non utilisés
- Sélection des composants logiciels, désactivation des utilitaires et paquetages non utilisés
- Gestion des comptes et privilèges d'administration
- Mises à jour des correctifs de sécurité
- Activation des traces d'audit
- Stratégie de sécurité (mot de passe, verrouillage)

[EXP_02] Documentation des procédures d'exploitation

Les procédures d'exploitation des systèmes informatiques sont documentées.

Cette documentation précise les instructions à suivre pour toute tâche qui relève de l'administration, de l'exploitation, de la supervision et de la maintenance des systèmes informatiques. Elle est tenue à jour, actualisée si nécessaire, et revue au minimum une fois par an.

[ISO 27001 - A 10.1.2]	Gestion des modifications

[EXP_03] Maîtrise des modifications et des configurations

Les configurations des systèmes informatiques et les modifications de ces systèmes font l'objet d'un contrôle strict. Une procédure précise les conditions de mise en œuvre des modifications.

Les impacts des modifications sont évalués et les changements testés. Les modifications importantes sont planifiées. Il convient de définir une procédure de repli.

Les configurations des Systèmes Informatiques sont documentées à l'aide d'outils adaptés. Tous les changements sont consignés sur un journal de bord indépendant des systèmes.

11.2. Administration des serveurs et des systèmes

[ISO 27001 - A 9.2.1]	Choix de l'emplacement et protection du matériel

[SRV_01] Installation et hébergement

Les serveurs sont installés en zone « machines », dans des locaux dédiés, sécurisés (contrôle d'accès, protection environnementale, télésurveillance) adaptés à la sensibilité des données qu'ils traitent et des informations qu'ils hébergent.

[SRV_02] Systèmes à priori sensibles

Les systèmes suivants sont automatiquement considérés comme sensibles et sont protégés :

- Contrôleurs de domaine, serveurs de nommage et serveurs d'annuaire.
- Serveurs antivirus
- Serveurs de messagerie
- Serveurs d'information interne (intranet, intradoc, …)
- Serveurs applicatifs sauf maquettes pédagogiques ou de recherche.
- Serveurs de fichiers, NAS, SAN et cloud
- Serveurs recevant des backups.

[SRV_03] Disponibilité des serveurs sensibles

Les serveurs d'infrastructure sont redondés dès que possible.

Il convient d'estimer la nécessité d'une redondance, d'un dispositif de secours ou d'un contrat de maintenance adapté en fonction des besoins

[ISO 27001 - A 11.5.1]	Ouverture de sessions sécurisées

[SRV_04] Administration et supervision

L'administration et la supervision des serveurs sont réalisées par des personnels autorisés depuis des environnements protégés (locaux, VLAN, consoles de supervision).

Les flux d'administration et de supervision sont protégés en confidentialité.

Les actions d'administration et de supervision sont tracées et font l'objet de revues périodiques.

[ISO 27001 - A 11.5.5]	Déconnexion automatique des sessions inactives

[SRV_05] Déconnexion automatique des sessions

Une période d'inactivité des sessions d'administration est définie pour les systèmes sensibles, au-delà de laquelle une nouvelle identification et une authentification sont rendues obligatoires.

[ISO 27001 - A 10.10.6]	Synchronisation des horloges

[SRV_06] Synchronisation des horloges

Afin de disposer d'un horaire fiable pour les traitements et la production de logs, les horloges de tous les ordinateurs sont synchronisées par une synchronisation automatique (NTP, rdate,…).

11.3. Systèmes d'impression

[ISO 27001 - A 10.8.5]	Systèmes d'information d'entreprise

[IMP_01] Protection de l'administration par mot de passe des imprimantes

Les fonctions d'administration locales ou distantes des imprimantes mutualisées qui reçoivent des données sensibles, sont protégées conformément à la gestion des comptes privilégiés et au contrôle d'accès logique aux équipements réseau (notamment en ce qui concerne le changement des mots de passe constructeurs.

[IMP_02] Configuration des imprimantes et des copieurs multifonctions

Les imprimantes et les copieurs sont configurés pour ne pas accepter de connexion locale (wifi, usb, …) sans mot de passe. Les mécanismes de stockage des données propres aux dispositifs mutualisés doivent être sécurisés pour éviter toute fuite de données. Cette disposition est indispensable en particulier dans le cadre des opérations de maintenance réalisées par un tiers (veiller aux clauses de confidentialité des contrats de maintenance).

[ISO 27001 - A 11.3.3]	Politique du bureau propre et de l'écran vide

[IMP_03] Protection des impressions

Des mesures organisationnelles permettent de limiter le temps de présence des impressions sensibles sur les imprimantes.

Les impressions sensibles (sujets d'examen par exemple) sont réalisées sur des imprimantes contrôlées (localisation physique protégée, imprimantes sur un réseau surveillé), et configurées pour ne permettre qu'au seul propriétaire des travaux ou aux agents des services de reprographie de pouvoir récupérer les impressions.

11.4. Surveillance et journalisation

[ISO 27001 - A 10.10.2]	Surveillance de l'exploitation du système

[SURV_01] Surveillance continue des systèmes

Chaque administrateur informatique assure une surveillance continue des systèmes et serveurs sous sa responsabilité.

Cette surveillance porte notamment sur :

- Le contrôle du bon fonctionnement du système d'exploitation.
- Le contrôle de la charge et de la disponibilité des systèmes et des serveurs.

- L'utilisation des systèmes d'information et des serveurs.

Cette surveillance s'appuie sur des moyens dédiés et protégés, qui sont éventuellement partagés avec ceux utilisés pour l'administration et l'exploitation des systèmes et des réseaux.

[ISO 27001 - A 10.10.4]	Journal administrateur et journal des opérations

[SURV_02] Journalisation des événements système

Les principaux événements liés à la sécurité sont enregistrés dans des fichiers de traces.

Cette journalisation porte notamment sur les événements suivants :

- Les anomalies pouvant être révélatrices d'un incident de sécurité.
- Les atteintes à la sécurité : détections de virus, tentatives d'intrusion, erreurs de connexion…
- L'activité des personnes en charge de l'exploitation du SI : configuration et paramétrage des systèmes, gestion des habilitations et des droits d'accès…
- L'activité « système » des utilisateurs : connexions et déconnexions, accès et utilisation des ressources.

Les journaux d'audit sont revus afin de détecter les problèmes de sécurité. Les événements révélateurs d'un possible problème de sécurité sont analysés quotidiennement. Ces dispositions sont conformes à la politique de gestion de gestion des journaux informatiques.

[SURV_03] Conformité des dispositifs de surveillance et de journalisation

Il convient de s'assurer que :

- les dispositifs de surveillance et de journalisation mis en œuvre soient conformes à la législation en vigueur, adaptés et proportionnels à l'enjeu et aux risques encourus.
- les informations journalisées respectent les exigences légales et réglementaires en matière de traces ainsi que pour la vie privée des utilisateurs.
- les instances représentatives des personnels sont consultées sur la mise œuvre de tels dispositifs et de la définition des modalités d'utilisation.
- les utilisateurs soient informés de leur mise en œuvre.

[ISO 27001 - A 10.10.3]	Protection des informations journalisées

[SURV_04] Conservation des journaux systèmes

Les journaux d'audit sont des biens sensibles, qui doivent être sauvegardés et protégés. Ils sont conservés pendant une période suffisante pour répondre aux besoins opérationnels et satisfaire les exigences légales, réglementaires ou contractuelles. Les systèmes de conservation sont contrôlés afin de vérifier la conformité à leur cahier des charges et à la politique de gestion des journaux informatiques.

12. Sécurité des applications et des données applicatives

12.1. Administration des applications

[ISO 27001 - A 11.1.1]	Politique de contrôle d'accès

[APP_01] Gestion des autorisations d'accès aux applications

Les autorisations d'accès aux applications (attribution d'un droit d'accès, révision, retrait) s'appuient sur des règles et procédures mises en place au titre du processus de gestion des habilitations et des droits d'accès.

Les droits alloués sont régulièrement réévalués.

[ISO 27001 - A 11.6.1]	Restriction d'accès à l'information

[APP_02] Contrôle d'accès aux applications

L'accès aux applications est contrôlé. Ce contrôle d'accès s'appuie sur les mécanismes mis en œuvre au titre de l'identification des utilisateurs, de leur authentification et des droits hérités de leur profil et du contexte d'utilisation.

Ces mécanismes conditionnent également l'accès aux différentes fonctions et aux différentes données au sein des applications.

L'accès alloué à un utilisateur est strictement personnel.

[ISO 27001 - A 10.10.2]	Surveillance de l'exploitation du système
[ISO 27001 - A 10.10.5]	Rapports d'anomalies

[APP_03] Contrôle et suivi de l'utilisation des applications

Il est souhaitable que les utilisations des fonctions applicatives soient tracées et journalisées (en fonction de leur sensibilité et des données accédées).

Les journaux applicatifs sont régulièrement analysés afin de détecter les erreurs d'utilisation, les dysfonctionnements et les utilisations illicites. L'utilisation d'un même identifiant pour l'accès à une application de gestion sur des postes différents doit être auditée et signalée à l'utilisateur et au responsable de l'application.

12.2. Sécurité des applications

[ISO 27001 - A 12.2.1]	Validation des données d'entrée
[ISO 27001 - A 12.2.2]	Mesure relative au traitement interne
[ISO 27001 - A 12.2.3]	Intégrité des messages
[ISO 27001 - A 12.2.4]	Validation des données de sortie

[APP_04] Validation des données et fonctions applicatives

Une vérification des données transmises aux applications sensibles est effectuée afin d'empêcher de porter atteinte à la sécurité des fonctions ou des informations des applications (valeurs hors intervalle, caractères invalides, données incomplètes, injections de code, etc…)

La conception et la mise en œuvre des applications doivent réduire les risques de pertes d'intégrité. Les droits de lecture, écriture, exécution sont ajustés au besoin.

En fonction de leur sensibilité, les applications alimentées en sources externes de données contrôlent l'intégrité des messages et données reçues.

Les tests de recettes des applications sont réalisés de manière systématique afin de s'assurer que les bonnes pratiques de sécurité ont été prises en compte.

[ISO 27001 - A 11.5.6]	Limitation du temps de connexion

[APP_05] Limitation de durée de connexion

Les applications sensibles, dont l'accès est réservé sur une plage horaire ou sur un accès de courte durée (applications accessibles depuis des zones difficilement contrôlables par l'Etablissement), mettent en œuvre des limitations du temps de connexion, par tranche horaire, par durée de connexion, ou par durée d'inactivité. Les utilisateurs doivent alors se ré-authentifier pour continuer l'usage de ces applications sensibles.

13. Sécurité de l'environnement utilisateur

13.1. Poste de travail

[ISO 27001 - A 7.1.1]	Inventaire des biens

[PDT_01] Attribution des postes de travail

L'attribution d'un poste de travail est soumise à autorisation par le responsable hiérarchique et en tenant compte des préconisations techniques du responsable informatique ; les usagers engagent leur responsabilité sur le respect des règles d'usage afférentes au poste (dont la charte du numérique).

[ISO 27001 - A 11.3.2]	Matériel utilisateur laissé sans surveillance
[ISO 27001 - A 8.2.2]	Sensibilisation, qualification et formations en matière de sécurité

[PDT_02] Rappel des règles de protection des postes de travail

Les principales règles et dispositions relatives à la sécurité des postes de travail et à leur utilisation sont rappelées dans la charte des usages numériques.

Elles sont également rappelées lors d'opérations périodiques de sensibilisation des utilisateurs.

Les utilisateurs sont sensibilisés à l'usage de moyens de protection physique des postes de travail en dehors de leur présence.

[PDT_03] Administration des postes de travail

Les équipes informatiques sont responsables de l'administration des postes de travail. En règle générale, l'utilisateur ne dispose pas des droits lui permettant de réaliser des opérations d'administration sur son poste de travail, si cela n'est pas justifié.

L'administration d'un poste de travail bureautique par son utilisateur reste une exception. Elle fait l'objet d'une demande formelle motivée et validée par la hiérarchie de l'utilisateur. L'administration peut-être déléguée aux utilisateurs dans le cadre des activités liées à la pédagogie ou à la recherche, avec l'accord de l'informaticien.

[PDT_04] Sécurité des postes de travail

Des mesures de sécurité sur les postes de travail bureautiques sont définies.

Ces mesures concernent à minima les conditions d'accès (identification et authentification obligatoires), l'intégrité du poste (outils anti-virus, droits d'administration), la disponibilité des informations (processus de sauvegarde). Les systèmes de verrouillage automatique des postes de travail ne doivent pas pouvoir être contournés par les utilisateurs.

[PDT_05] Configuration type sécurisée

Une ou des configurations destinées à l'installation des postes de travail sont définies en intégrant les règles et bonnes pratiques de sécurité. La définition de ces configurations et notamment les arbitrages relatifs à leur sécurisation est validée par le responsable informatique.

13.2. Supports informatiques mobiles

[ISO 27001 - A 10.7.1]	Gestion des supports amovibles

[PDT_06] Usage des supports d'information amovibles et mobiles.

Les utilisateurs sont sensibilisés sur les risques de leur utilisation au sein de l'établissement (introduction de virus, divulgation d'information en cas de perte ou vol) et appliquent les consignes.

[PDT_07] Stockage d'une information sensible sur support amovible ou mobile

Dès lors qu'elles sont stockées sur un support amovible ou mobile, les informations sensibles font l'objet d'une protection ou d'un chiffrement appropriés.

[ISO 27001 - A 10.7.2]	Mise au rebut des supports

[PDT_08] Mise au rebut des supports amovibles

Les supports de données mobiles ou amovibles (disques durs, clés USB, etc…) sont considérés comme des biens sensibles et sont par conséquent soumis aux procédures de destructions de ce type de biens.

13.3. Téléphonie

[PDT_09] Sécurisation des autocommutateurs

Les autocommutateurs doivent être maintenus à jour au niveau des correctifs de sécurité. Leur configuration doit être durcie. La définition et l'affectation des droits d'accès et des privilèges aux utilisateurs (transfert départ-départ, entrée en tiers, interphonie, autorisation de déblocage, renvoi sur numéro extérieur, substitution, substitution de privilège, interception d'appel dirigé, etc.) doivent faire l'objet d'une attention particulière. Une revue de la programmation téléphonique doit être organisée périodiquement.

[PDT_10] Sécurisation des codes d'accès

Il est nécessaire de sensibiliser les utilisateurs au besoin de modifier le code d'accès de leur téléphone et de leur messagerie vocale.

[PDT_11] Utilisation du DECT

Les communications réalisées au travers du protocole DECT sont susceptibles d'être interceptées, même si les mécanismes d'authentification et de chiffrement que propose ce protocole sont activés. Il est recommandé d'attribuer des postes téléphoniques filaires aux utilisateurs dont les échanges sont les plus sensibles

13.4. Bureautique

[ISO 27001 - A 10.8.5]	Systèmes d'information d'entreprise

[BUR_01] Sécurité des documents bureautiques utilisateurs

L'ensemble des espaces de stockage mis à la disposition de chaque utilisateur par la DSI, dédié en particulier à la bureautique, **est sécurisé et sauvegardé sans intervention de l'utilisateur**. L'accès à ces espaces utilisateurs sécurisés est limité à l'utilisateur et aux administrateurs autorisés.

[BUR_02] Sécurité des espaces bureautiques partagés (groupware)

Des espaces bureautiques partagés sécurisés et sauvegardés sont créés à la demande (pour des projets, des applications bureautiques). L'accès à ces espaces partagés est sous le contrôle d'un responsable identifié.

Les documents bureautiques confidentiels partagés sont stockés dans des espaces partagés sécurisés, archivés et automatiquement sauvegardés sans intervention de l'utilisateur.

13.5. Messagerie

[ISO 27001 - A 10.8.4]	Messagerie électronique

[MES_01] Formalisation des règles d'utilisation de la messagerie électronique

Les règles relatives à l'utilisation de la messagerie sont formalisées et mises à la disposition des utilisateurs. Elles sont rappelées dans la charte de la messagerie électronique.

[MES_02] Contrôle d'accès à la messagerie électronique

L'accès à la messagerie nécessite une identification et une authentification préalables de l'utilisateur. Un protocole chiffré est mis en place sur tout le processus de consultation des messages.

[MES_03] Analyse des messages

Les messages électroniques sont systématiquement analysés au niveau antispam et antivirus soit par Renater soit sur les ressources de la DSI. Les dispositifs employés sont d'une technologie différente de celle employée sur les postes de travail. Les messages comportant un virus ou étant manifestement du spam sont bloqués par le serveur.

[MES_04] Signature et chiffrement des messages et pièces jointes

La messagerie de l'établissement fournit des mécanismes de signature et de chiffrement des messages.

Les utilisateurs ayant besoin d'échanger des fichiers sensibles disposent sur leur poste de travail d'un logiciel de chiffrement de fichiers, certifié par l'ANSSI.

14. Mobilité

14.1. Sécurité des postes nomades

[ISO 27001 - A 11.7.1]	Informatique mobile et télécommunications
[ISO 27001 - A 9.2.5]	Sécurité du matériel hors des locaux

[NOMAD_01] Politique de sécurité des postes nomades

Un document d'application spécifique à la mobilité est défini. Il traite a minima les points suivants :

- Ouverture de session protégée par mot de passe,
- obligation d'un mode d'accès sécurisé (VPN) pour l'accès au réseau interne (service exclusivement réservé aux machines de l'Université),
- utilisation de moyens de chiffrement des données sur les postes nomades de l'Université,
- rappel des risques de connexion sur des moyens non sûrs avec ses identifiants universitaires (cybercafé, hotspot, …)

[NOMAD_02] Attribution d'un accès nomade – formulaire d'engagement

Toute infrastructure d'accès distants est soumise à autorisation de la DSI et du RSSI. L'attribution d'un accès sécurisé nomade (VPN) est soumis suivant le cas à la DSI ou au responsable de l'infrastructure informatique locale, sur demande écrite du responsable hiérarchique.

Les usagers autorisés signent un formulaire d'engagement au travers duquel ils reconnaissent leurs responsabilités et affirment leur connaissance des règles d'usage afférentes au moyen d'accès nomade. L'accès est donné pour une période limitée dans le temps et fixée à l'ouverture. Une revue annuelle des droits d'accès est organisée par la DSI et le RSSI

Toute autorisation d'accès fait l'objet d'une inscription au registre ad-hoc.

14.2. Utilisation de matériel hors des locaux

[ISO 27001 - A 9.2.5]	Sécurité du matériel hors des locaux

[NOMAD_03] Dispositifs de sécurité installés sur les nomades

Tout poste nomade comprend par défaut :

- Un système de protection contre les logiciels malveillants.
- Un logiciel de chiffrement de disque et/ou des fichiers (certifié par l'ANSSI).

Selon les besoins identifiés et les informations traitées, des configurations durcies peuvent être mises à disposition des usagers : authentification forte pour la connexion au poste, outil de chiffrement des disques durs, support amovible sécurisé, outil de contrôle de double connexion LAN/VPN.

[NOMAD_04] Utilisation des postes nomades à l'extérieur

Les utilisateurs s'appuient sur le « passeport de conseils aux voyageurs » de l'ANSSI.

[NOMAD_05] Mises à jour et correctifs de sécurité des postes nomades

Les postes nomades doivent être configurés pour installer les correctifs et les mises à jour automatiquement. S'il s'agit de postes dédiés au prêt, ils doivent être ré-initialisés à chaque changement d'emprunteur.

Une procédure est mis en place afin de s'assurer que les mises à jour et correctifs de sécurité des postes nomades sont systématiquement exécutés avant leur reconnexion au réseau interne de l'établissement.

14.3. Télétravail

[ISO 27001 - A 11.7.2]	Télétravail

[NOMAD_06] Télétravail

Dans le cadre de la politique de télétravail de l'établissement, un document précise les modalités des connexions distantes au SI et l'utilisation de cette connexion. L'autorisation d'accès est à adresser au DSI et au RSSI de l'Université.

Il est rappelé que l'utilisation de PC ou de terminaux personnels est interdite sans dérogation préalable en dehors des réseaux ou zones prévues à cet effet. Le télétravail comme le traitement ou le stockage de données, qui sont la propriété de l'établissement, ne peuvent être réalisés que sur les équipements mis à la disposition des utilisateurs par l'établissement.

15. Antivirus

15.1. Codes malveillants

[ISO 27001 - A 10.4.1]	Mesures contre les codes malveillants

[VIR_01] Existence d'une politique antivirale

Le responsable informatique met en œuvre une politique antivirale permettant de protéger les systèmes contre les virus et tout autre type de logiciels malveillants connus. Des procédures sont définies afin de gérer et circonscrire les attaques virales. Ce choix d'outil est conforme à la politique de l'établissement.

[VIR_02] Disponibilité et utilisation quotidienne des antivirus

La DSI met à disposition un ensemble de serveurs antivirus officiel éventuellement relayé en proximité. Tout poste compatible doit s'y rattacher.. Chaque responsable informatique peut prendre toutes les mesures complémentaires qu'il estime nécessaires. Celles-ci ne doivent pas conduire à un blocage des communications internes à l'UCA et ne doivent pas recourir à un système de filtrage externe au réseau RENATER sans accord préalable de la DSI. Il est du devoir de chaque administrateur système de partager les bonnes pratiques dans ce domaine.

Il est de la responsabilité de chaque administrateur système de s'assurer que tout équipement concerné dispose d'un antivirus actif et à jour et qu'un scan a lieu régulièrement. Les consoles centrales doivent être surveillées quotidiennement. . Les systèmes de type UNIX hébergeant des données à destination de machines non UNIX (Microsoft, Apple) doivent comporter un anti-virus à jour permettant d'éviter l'effet porteur sain.

Les systèmes de stockage de type cloud doivent respecter les prescriptions des deux paragraphes ci-dessus.

[VIR_03] Détection et traitement des virus

Tout virus détecté déclenche automatiquement une mise en quarantaine des fichiers concernés. Si la machine s'avère infectée elle devra être remise en conformité par une procédure permettant de garantir l'absence de propagation. Les éventuels fichiers utilisateurs devront être réimplantés après un scan systématique.

S'il s'avère qu'une machine a été infectée bien qu'elle soit gérée de façon conforme aux prescriptions du [VIR_02], une information des équipes concernées, du RSSI et de la DSI doit être réalisée. Les enregistrements des journaux concernant les détections doivent être analysés de façon à ce que la ou les sources éventuelles de virus soient éradiquées.

16. Projet, développement et maintenance

16.1. Sécurité dans les projets du SI

La sécurité est prise en compte à toutes les étapes du cycle de vie d'un projet, interne ou externe, lié au système d'information. Les applications informatiques sont sécurisées, en cohérence avec la sensibilité des informations traitées et échangées.

16.1.1. Analyse et spécification

[ISO 27001 - A 10.3.1]	Dimensionnement
[ISO 27001 - A 12.1.1]	Analyse et spécification des exigences de sécurité

[PDM_01] Étude et dossier de sécurité

Une identification préalable des projets sensibles (manipulant soit des données sensibles, soit des données personnelles, soit présentant de forts besoins de disponibilité) est réalisée pour identifier les enjeux et les risques.

[ISO 27001 - A 12.5.5]	Externalisation du développement logiciel

[PDM_02] Acquisition de solutions et externalisation des développements

Les cahiers des charges rédigés pour l'acquisition d'une solution sensible (produit, système ou service) ou son développement tiennent compte de l'analyse de sécurité et incluent des clauses qui formulent les exigences et les conditions d'emploi prévues.

Ces cahiers des charges doivent inclure aussi des clauses destinées à assurer la pérennité de ces solutions et prendre en compte la maintenance et les contraintes d'évolution des systèmes et logiciels support dues à la mise en place de correctifs.

16.1.2. Développement

[ISO 27001 - A 12.5.1]	Procédures de contrôle des modifications
[ISO 27001 - A 12.2.1]	Validation des données d'entrée
[ISO 27001 - A 12.2.3]	Intégrité des messages

[PDM_03] Fonctions et services de sécurité

Les fonctions et services de sécurité qu'il convient de mettre en œuvre pour couvrir les exigences et les mesures retenues sont au minimum :

- L'utilisation de la notion de profil métier pour le contrôle d'accès
- La journalisation des accès et de l'utilisation des différentes fonctions applicatives
- Le contrôle des données d'entrée et des procédures de saisie
- La mise en place de mécanismes de reprise et de gestion des erreurs
- La sécurisation ou le durcissement des équipements, des systèmes et des configurations
- La mise en œuvre des derniers correctifs ou la demande de dérogation dans les cas où ce n'est pas possible
- La capacité de sauvegarder et de restaurer les données applicatives

16.1.3. Sécurité du développement et de la maintenance (processus et environnement)

[ISO 27001 - A 10.1.4]	Séparation des équipements de développement, de test et d'exploitation

[PDM_04] Cloisonnement des environnements

Les environnements de développement et de maintenance, de test et de pré-production sont distincts de l'environnement exploitation.

Les données utilisées pour le développement et les tests ne sont jamais des données opérationnelles sensibles.

[PDM_05] Gestion des sources, des évolutions et des modifications

Les programmes sources, les scripts et les fichiers de paramètres sont gérés par un système de gestion de versions.

L'accès à ce service comme aux données utilisées pour le développement est protégé.

16.2. Suivi d'exploitation

[ISO 27001 – A 10.3.1]	Dimensionnement

[PDM_06] Bon fonctionnement des applications

Les applications sensibles sont hébergées sur des serveurs récents, dont la maintenance « constructeur » est toujours assurée. Il en va de même pour les systèmes d'exploitation. Dans le cas particulier des systèmes libres, sont utilisées soit des versions stables (LTS) soit validées par l'éditeur.

[ISO 27001 - A 10.10.1]	Rapport d'audit
[ISO 27001 - A 10.10.2]	Surveillance de l'exploitation du système
[ISO 27001 - A 10.10.3]	Protection des informations journalisées
[ISO 27001 - A 10.10.4]	Journal administrateur et journal des opérations

[PDM_07] Politique de journalisation

Cf document : La politique de gestion des journaux informatiques.

16.3. Maintenance et mises à jour

[ISO 27001 - A 10.1.1]	Procédures d'exploitation documentées

[MAINT_01] Gestion et contrôle des opérations de maintenance

Les opérations de maintenance sont documentées (périmètre, actions…) et planifiées en concertation avec la DSI et les utilisateurs.

Des mesures sont prises (par exemple des tests de non régression) pour vérifier que l'opération de maintenance réalisée n'a pas altéré le système opérationnel.

Un retour en arrière en cas de dysfonctionnement constaté ou d'altération des données faisant suite à l'opération de maintenance réalisée doit toujours être possible.

Les opérations de maintenance effectuées localement par une société extérieure sont réalisées sous le contrôle permanent d'un agent de l'établissement. Les opérations effectuées au titre des opérations de maintenance sont tracées et journalisées. Un compte-rendu des opérations est systématiquement rédigé.

[ISO 27001 - A 11.7.1]	Informatique mobile et télécommunications

[MAINT_02] Télémaintenance

Les services de télémaintenance sont systématiquement encadrés par des accords contractuels qui précisent les conditions dans lesquelles sont effectuées les opérations de télémaintenance.

Les accès de télémaintenance (comptes dédiés, accès réseau) sont fermés en dehors des périodes de télémaintenance. Ils sont ouverts à la demande des télémainteneurs et à l'initiative des exploitants du système télémaintenu et sont fermés à la fin de toute opération de télémaintenance.

Il convient de s'assurer, via les conditions d'emploi, que les télémainteneurs informent systématiquement les exploitants de la fin de chaque opération de maintenance afin de leur permettre de fermer les accès.

Les opérations de télémaintenance sont tracées et journalisées. Elles font l'objet d'un contrôle a posteriori systématique.

16.4. Gestion des changements

Par changements, on entend les évolutions du SI traitées par les équipes chargées de l'exploitation.

Ces évolutions concernent principalement l'infrastructure support du SI : évolutions matérielles, évolutions logicielles, mises à jour des configurations, etc.

[ISO 27001 - A 10.1.2]	Gestion des modifications
[ISO 27001 - A 12.4.1]	Mesure relative aux logiciels en exploitation

[GCH_01] Procédure de gestion des changements

Un plan pluriannuel de renouvellement du matériel d'infrastructure SI gestion, SI communication et réseau est formalisé.

[GCH_02] Mise en œuvre des évolutions logicielles majeures

Les évolutions logicielles majeures sont planifiées. Elles sont testées avant leur mise en œuvre effective. Une procédure de repli est systématiquement définie. Toute évolution prévue n'est réalisée qu'une fois les procédures ci-dessus décrites par écrit. Les changements impactant doivent faire l'objet d'une communication suffisamment tôt.

[GCH_03] Contrôle et suivi

Toute évolution dans un sous-système du SI fait l'objet d'une inscription dans le journal de bord associé.

16.5. Gestion des vulnérabilités techniques et des correctifs

Un processus permet d'être informé en temps voulu de toute vulnérabilité technique relative aux systèmes d'information en exploitation, d'évaluer l'exposition du SI vis-à-vis de ces vulnérabilités et d'entreprendre les actions appropriées pour traiter le risque associé.

[ISO 27001 - A 12.6.1]	Mesure relative aux vulnérabilités techniques

[VULN_01] Dispositif de veille et d'évaluation des vulnérabilités

Une structure de veille permet d'être informé en temps voulu des vulnérabilités exceptionnellement dangereuses et des correctifs publiés par les éditeurs ou les sites autorisés (par exemple, les CERT).

Chaque administrateur systèmes et réseaux assure la veille dans le périmètre qui le concerne.

La criticité de chaque vulnérabilité (i.e. l'impact qui résulterait de leur exploitation) et de chaque correctif (c'est-à-dire des vulnérabilités corrigées) est évaluée localement ainsi que les actions à entreprendre. Cette évaluation inclut une détermination du niveau d'urgence de ces actions, sous la responsabilité des administrateurs systèmes et réseau locaux.

Les corrections de failles de sécurité critiques sur des serveurs sensibles et exposés doivent être réalisées dès qu'elles sont connues.

L'application des autres correctifs de sécurité donne lieu à une analyse évaluant le niveau d'urgence et les impacts des modifications sur la continuité de service.

[VULN_02] Gestion des mises à jour et correctifs

Des mesures permettent de s'assurer de l'authenticité des mises à jour et des correctifs reçus ou téléchargés. En particulier, ceux concernant les « produits du commerce » sont uniquement obtenus des sites des éditeurs ou de sites sûrs (CERT). Leur intégrité est systématiquement contrôlée.

Dans le cas des systèmes et applications sensibles, les mises à jour et correctifs sont systématiquement testés et validés préalablement à leur installation par mise en œuvre dans des environnements de test représentatifs des environnements de production. Ces tests comprennent des tests de compatibilité avec l'existant et des tests de non régression.

Les mises à jour et correctifs sont appliqués dans des délais cohérents avec leur niveau de criticité et leur niveau d'urgence. La bonne application des correctifs est contrôlée et mesurée, en particulier sur les postes des utilisateurs.

16.6. Fin de vie des projets

[ISO 27001 - A 9.2.6]	Mise au rebut ou recyclage sécurisé(e) du matériel

[PDM_08] Mise au rebut et recyclage en fin de projet

Une procédure décrit les précautions à prendre lors de la mise au rebut ou du recyclage de tout support d'information.

Il convient de s'assurer de :

- La destruction sécurisée des documents relatifs au projet après leur archivage numérique.
- De l'effacement sécurisé ou de la destruction physique des disques durs et des supports informatiques. La destruction doit être réalisée conformément aux préconisations de la clause « destruction des biens sensibles de cette PSSI ».

[PDM_09] Réaffectation des matériels en fin de projet

Préalablement au recyclage, à l'attribution à un nouveau propriétaire ou à la réaffectation d'un poste de travail ou d'un équipement matériel, tout le système et les données sont effacés avec les outils adéquats. Un archivage et une sécurisation de ces données peuvent être réalisés au préalable si nécessaire.

17. Sauvegarde et archivage

[ISO 27001 - A 10.5.1]	Sauvegarde des informations

[SAU_01] Politique de sauvegarde

Une politique de sauvegarde est formalisée, qui tient compte d'une part des besoins de sécurité des données, des contraintes techniques et du cadre règlementaire.

Cette politique de sauvegarde est revue au minimum une fois par an et mise à jour lors de toute évolution du système d'information.

[SAU_02] Plan de sauvegarde

Un Plan de Sauvegarde est formalisé en cohérence avec le Plan de Continuité d'Activité, qui décrit les opérations de sauvegarde des données. Ce plan de sauvegarde est adapté aux différents type de données (exemple données utilisateurs, données applicatives, courriers électroniques, applications et systèmes, …)

Pour chaque donnée ou ensemble de données, les besoins de sauvegarde sont établis en considérant :

- Les obligations légales, réglementaires ou contractuelles en matière de sauvegarde ou d'archivage ;
- Le temps maximal d'indisponibilité admissible, qui détermine la durée maximale pour la restauration des données et du service à partir d'une sauvegarde ;
- La perte maximale de données admissible et d'usage de l'application, qui permettront de déterminer la politique de sauvegarde (périodicité, mode opératoire).

[SAU_03] Exigences génériques

Le plan de sauvegarde définit les conditions de sauvegarde afin de garantir une perte de données minimale en cohérence avec les besoins exprimés par les responsables d'applications.

[SAU_04] Test des sauvegardes

Le bon déroulement des sauvegardes est validé avant stockage des supports; cette validation est effectuée soit par les moyens techniques fournis par le système de sauvegarde s'ils le permettent, soit par des vérifications manuelles.

Le volume de données sauvegardées doit être suivi par les équipes d'exploitation, pour anticiper les problèmes liés à la capacité des supports.

[SAU_05] Restauration

Les procédures de restauration sont documentées. Des tests de restauration sont effectués au minimum 2 fois par an et les résultats de ces tests sont conservés.

Il convient que des moyens de restauration soient également disponibles hors du site sauvegardé pour pouvoir restaurer les données en cas d'incident ayant détruit le système d'origine.

[SAU_06] Gestion et protection des supports de sauvegarde

Les supports de sauvegarde sont conservés dans des locaux sécurisés ou des armoires fortes adaptés à leur niveau de sensibilité (équivalent à celui des données sauvegardées). Il convient que ces locaux soient suffisamment éloignés des systèmes sauvegardés pour éviter toute destruction simultanée des données et de leurs sauvegardes notamment par un incendie. Il convient d'utiliser de préférence des armoires ignifugées.

L'accès à ces locaux ou armoires fortes est limité à un nombre restreint de personnes autorisées.

[SAU_07] Externalisation des sauvegardes

En cas d'externalisation des sauvegardes (prestataire), il convient de s'assurer par contrat que les ressources et services fournis par le prestataire sont conformes aux besoins exprimés par

l'établissement, notamment du point de vue de la confidentialité. La mise en œuvre effective des mesures de sécurité par le prestataire est contrôlée régulièrement.

18. Gestion des incidents

18.1. Organisation et procédure

[ISO 27001 - A 13.2.1]	Responsabilités et procédures

[INC_01] Procédure de gestion des incidents

L'Établissement met en œuvre une gestion des incidents liés à la sécurité, centralisée au niveau du RSSI de l'Etablissement. Une organisation et des procédures sont définies, et traitent les aspects :

- identification et caractérisation des incidents ;
- processus de signalement des incidents ;
- confinement de l'incident ;
- analyse des incidents (cause, contexte), collecte de traces d'audit ;
- planification des actions correctrices
- formalisation des incidents dans un référentiel unique (identification, date, circonstances, actions correctrices et références documentaires, comptes rendu) ;
- établissement de fiches réflexe (réaction face à un incident connu) ;
- incidents récurrents : prévoir un projet d'actions préventives ;
- communication (interne et externe) et sensibilisation auprès des personnels.

Dans le cas d'incidents majeurs (impliquant éventuellement des tiers extérieurs ou des partenaires) nécessitant une expertise technique, le CPSSI nomme un comité d 'experts chargés de produire un rapport sur l'incident.

Tout incident de sécurité doit être déclaré immédiatement au RSSI.

[ISO 27001 - A 13.2.2]	Exploitation des incidents liés à la sécurité de l'information déjà survenus

[INC_02] Retour d'expérience

Tout incident de sécurité nécessite d'être analysé afin d'identifier les faiblesses exploitées et définir si nécessaire les mesures correctives permettant d'en limiter la répétition.

[ISO 27001 - A 13.2.3]	Collecte de preuves

[INC_03] Conservation des traces

Tout incident de sécurité peut conduire à des sanctions, nécessiter des actions en justice ou conduire à un contentieux contractuel.

Les traces et les éléments susceptibles de servir de preuve, comme de permettre une analyse à posteriori des incidents, sont recueillis et conservés en lieu sûr.

Pour toute question concernant la conservation des traces, il convient de se référer au document « Politique de gestion des journaux informatisés » de l'Etablissement.

18.2. Surveillance et signalement des incidents

[ISO 27001 - A 13.1.1]	Signalement des événements liés à la sécurité de l'information
[ISO 27001 - A 13.1.2]	Signalement des failles de sécurité

[INC_04] Procédure de signalement

Il appartient au RSSI de définir et mettre en place une procédure formelle et documentée de remontée d'information et de signalement des événements et failles susceptibles d'avoir une incidence sur la sécurité des biens de l'Établissement.

[INC_05] Surveillance du SI et détection des incidents

Des moyens organisationnels et des outils de supervision permettent un suivi de l'activité au niveau du système d'information et la détection des incidents :

- Supervision des éléments réseau et systèmes critiques sur le plan de la sécurité. Journalisation en temps réel des évènements liés à la sécurité du système d'information.

Il appartient aux équipes informatiques :

- De réaliser une surveillance continue des systèmes et des réseaux et de revoir périodiquement les différents journaux à la recherche d'anomalies pouvant être révélatrices d'incidents.
- D'analyser et traiter les anomalies détectées. Ces analyses doivent être formalisées et conservées, les alertes transmises au RSSI.

[INC_06] Information et sensibilisation du personnel

Il appartient à chaque responsable de s'assurer que chacun, personnel ou contractant, est sensibilisé et connaît la procédure de signalement des incidents.

Le CPSSI, est chargé de définir un plan d'information et de sensibilisation du personnel et de s'assurer de la mise en œuvre de cette sensibilisation par la direction des ressources humaines.

[INC_07] Signalement des incidents par le personnel

Le personnel de l'Établissement est tenu de signaler, le plus rapidement possible, tout événement ou faille de sécurité pouvant impacter la sécurité à l'informaticien de sa structure (ou directement au RSSI en cas d'absence).

19. Gestion du plan de continuité d'activité

19.1. Organisation

[ISO 27001 - A 14.1.1]	Intégration de la sécurité de l'information dans le processus de gestion du plan de continuité de l'activité

[PCA_01] Organisation du PCA (Plan de Continuité d'Activité).

L'Établissement met en place une organisation permettant de répondre aux incidents majeurs pour revenir rapidement à un état fonctionnel acceptable.

Les rôles et responsabilités des intervenants dans le cadre du Plan de Continuité d'Activité (PCA) sont identifiés, ainsi que les astreintes associées. Les modalités de déclenchement du PCA sont définies.

19.2. Formalisation

[ISO 27001 - A 14.1.2]	Continuité de l'activité et appréciation du risque
[ISO 27001 - A 14.1.3]	Élaboration et mise en œuvre des plans de continuité intégrant la sécurité de l'information
[ISO 27001 - A 14.1.4]	Cadre de la planification de la continuité de l'activité

[PCA_02] Existence du PCA sur les ressources de l'établissement.

L'Établissement dispose d'un Plan de Continuité d'Activité (PCA) permettant de palier tout arrêt prolongé des systèmes et applications critiques.

Ce PCA définit notamment :

- Les moyens mis en œuvre et les modalités opérationnelles permettant d'assurer la continuité des fonctions vitales de l'établissement suite à une situation de crise ;
- Les rôles et les activités de chacun ;
- Les modalités de basculement en mode dégradé ou sur les solutions de secours.

[PCA_03] Mise à jour du PCA

L'intégration d'une nouvelle application dans le système d'information fait l'objet d'une mise à jour du plan de continuité d'activité le cas échéant.

[PCA_04] Existence du site de secours

L'Établissement met en place un site de secours, pour ses applications et informations les plus critiques, qui permet le redémarrage des services critiques dans les délais convenus et dans le cadre de son PRA (Plan de Reprise d'Activité).

19.3. Test

[ISO 27001 - A 14.1.5]	Mise à l'essai, gestion et appréciation constante des plans de continuité de l'activité

[PCA_05] Test du PCA

Le plan de continuité d'activité est testé et validé régulièrement avec une fréquence définie par le CPSSI.

20. Conformité et contrôle

20.1. Conformité avec les exigences légales et réglementaires

[ISO 27001 - A 15.1.1]	Identification de la législation en vigueur

[CONF_01] Conformité avec les exigences légales et réglementaires

Les procédures de sécurité, ainsi que leurs mises à jour, sont établies dans le respect des obligations légales, règlementaires et contractuelles.

[CONF_02] Identification de la législation en vigueur

Une veille est assurée par le responsable juridique afin d'identifier les lois et règlements nationaux auxquels le SI de l'Établissement se conforme. Ces lois et règlements sont répertoriés et documentés. Les intervenants sont régulièrement informés au travers du CPSSI.

[*ISO 27001 - A 15.1.2]*	Droits de propriété intellectuelle

[CONF_03] Respect des droits de propriété intellectuelle

L'Établissement dispose de règles et procédures appropriées visant à garantir le respect de la propriété intellectuelle tant pour les biens possédés ou confiés à l'Établissement que pour les droits détenus par l'Établissement.

En particulier :

- L'Établissement s'engage à acquérir les logiciels uniquement à partir de sources connues et réputées.
- Les licences originales et les preuves d'achats des matériels et logiciels utilisés sont conservées en lieu sûr par le responsable de l'installation.
- Des contrôles sont régulièrement effectués afin de vérifier le respect de la législation et de régulariser les licences globales. En cas de manquement caractérisé, des sanctions peuvent être prise à l'encontre des contrevenants.

[ISO 27001 - A 15.1.3]	Protection des enregistrements de l'organisme

[CONF_04] Obligation de protection des enregistrements de l'organisme

Des mesures organisationnelles et techniques sont définies et mises en place afin de protéger les enregistrements importants sur un plan légal ou réglementaire (journaux de log, activités des dispositifs de contrôles d'accès, archives de vidéosurveillance) contre une perte, destruction ou falsification, conformément aux exigences légales et réglementaires et aux contraintes métier.

[ISO 27001 - A 15.1.4]	Protection des données et confidentialité des informations relatives à la vie privée

[CNIL_01] Protection des données à caractère personnel

L'établissement prend en compte les exigences du Règlement Général de la Protection des Données (RGPD) relatif à la protection des données à caractère personnel. Il mène en particulier les les actions suivantes :

- Lister les traitements de données personnelles
- Mettre en œuvre les actions d'information et de sensibilisation des acteurs concernés par les traitements d'informations personnelles
- Formaliser les directives internes et les procédures
- Mettre en place une démarche de gestion des risques
- Contractualiser avec les partenaires et les sous-traitants
- S'assurer de l'effectivité des mesures de sécurité sur les traitements, garantissant la confidentialité des données

Le Délégué à la Protection des Données (DPD) de l'université est chargé de surveiller l'application du RGPD et tient à jour le registre de l'Université dans ce domaine.

[CNIL_02] Déclaration des traitements

Tout nouveau projet traitant de données à caractère personnel fait l'objet d'une information auprès d'un correspondant CNIL (CIL) ou du Le Délégué à la Protection des Données (DPD) lorsqu'il est désigné..

[ISO 27001 - A 15.1.5]	Mesure préventive à l'égard du mauvais usage des moyens de traitement de l'information

[CNIL_03] Communication sur la protection des données à caractère personnel

Tout responsable qui souhaite mettre en œuvre un traitement de données personnelles doit préalablement contacter le CIL via l'application prévue à cet effet, afin de déterminer les formalités à accomplir et les mesures à mettre en œuvre pour protéger les informations traitées.

20.2. Conformité avec les politiques et normes, conformité technique

[ISO 27001 - A 15.2.1]	Conformité avec les politiques et les normes de sécurité
[ISO 27001 - A 15.2.2]	Vérification de la conformité technique

[VULN_03] Analyses de vulnérabilités

Des analyses de vulnérabilités peuvent être réalisées si nécessaire. Ces analyses de vulnérabilités couvrent notamment les aspects suivants:

- L'exploration des possibilités d'accès depuis un poste de travail banalisé connecté depuis les différents réseaux internes de l'Établissement.
- L'exploration des possibilités d'accès à l'infrastructure SI de l'Établissement depuis un système connecté au réseau Internet et ne disposant d'aucune autorisation particulière.

Les résultats de ces tests de vulnérabilités sont analysés. Les vulnérabilités identifiées font l'objet d'un plan d'action afin de corriger ces vulnérabilités ou d'y pallier à plus ou moins long terme en fonction de leur criticité.

Afin d'éviter tout effet nuisible les administrateurs systèmes et réseaux des machines auditées sont prévenus avant la réalisation de l'audit.

20.3. Processus d'audits internes et externes

[ISO 27001 - A 15.3.1]	Contrôles de l'audit du système d'information

[AUD_01] Contrôle et suivi

Le CPSSI fait effectuer un contrôle annuel du suivi des règles de sécurité sur autant de projets opérationnels représentatifs qu'il le juge nécessaire.

[AUD_02] Réalisation des audits

Des contrôles et tests sur la base d'audit pourront être réalisés Les audits visent à s'assurer de l'effectivité de la mise en œuvre des mesures de sécurité, et d'évaluer leur efficacité.

Les audits portent sur les aspects documentaires liés à la sécurité du SI (procédures) les aspects techniques (mesures) et sur les aspects organisationnels.

Des mesures organisationnelles sont prises de manière à documenter toutes les procédures, exigences et responsabilités nécessaires à la bonne réalisation de l'audit. La DSI met à disposition les ressources destinées à l'exécution de ces contrôles.

[AUD_03] Analyse des résultats d'audit

Les résultats des audits sont analysés afin de pouvoir réviser et améliorer les procédures et les mesures de sécurité.

[ISO 27001 - A 15.3.2]	Protection des outils d'audit du système d'information

[AUD_04] Protection des outils d'audit

Les outils d'audit (logiciels ou fichiers de données) sont séparés des systèmes en exploitation et ne sont accessibles que par les personnes autorisées.

Annexe 1

21. Livrables attendus mentionnés dans la présente politique :

- Plan de classification des biens
- Procédure de mise au rebut des biens
- Chartes d'usage et de sécurité des systèmes d'information (charte des usages des ressources numériques dite charte numérique, charte des administrateurs techniques, charte des équipements nomadisme, messagerie électronique, …)
- Plan d'infrastructure des bâtiments et mesures de sécurité physiques
- Procédure de gestion des habilitations, des profils et des droits d'accès (physiques et logiques)
- Politique de gestion des authentifiants
- Politique de sauvegarde
- Plan de sauvegarde
- Documents d'architecture réseau
- Politique de contrôle et filtrage des flux réseaux
- Plan de Continuité d'Activité
- Plan de Reprise d'Activité
- Note de sécurité relative à l'usage des mots de passe
- Document d'autorisation de suppression du compte et des données après le départ
- Procédure de gestion des comptes utilisateurs
- Politique de gestion des journaux informatiques
- Politique de sécurité des postes nomades
- Accès nomade, formulaire d'engagement des utilisateurs pour les accès nomades
- Passeport de conseil aux voyageurs de l'ANSSI Politique antivirale [VIR_01]
- Procédure de gestion des incidents

UNIVERSITÉ Clermont Auvergne

CHARTE DES ADMINISTRATEURS TECHNIQUES

Université Clermont Auvergne

Table des matières

1. Contexte et définitions

Introduction

La présente charte complète la charte générale relative aux usages numériques de l'université Clermont Auvergne (ci-après « la charte générale »), et définit spécifiquement le cadre d'intervention de l'administrateur technique. Les deux chartes s'appliquent donc conjointement aux administrateurs techniques.

Pour les besoins de sa mission, l'administrateur technique détient le plus haut niveau d'autorisations sur le ou les systèmes qu'il administre. Il se différencie de l'administrateur fonctionnel qui lui intervient sur les applications à travers les écrans de gestion.

Afin de protéger l'administrateur technique, de protéger l'établissement et ses usagers d'agissements contraires à leurs intérêts, la présente charte formalise les droits et devoirs de l'administrateur technique.

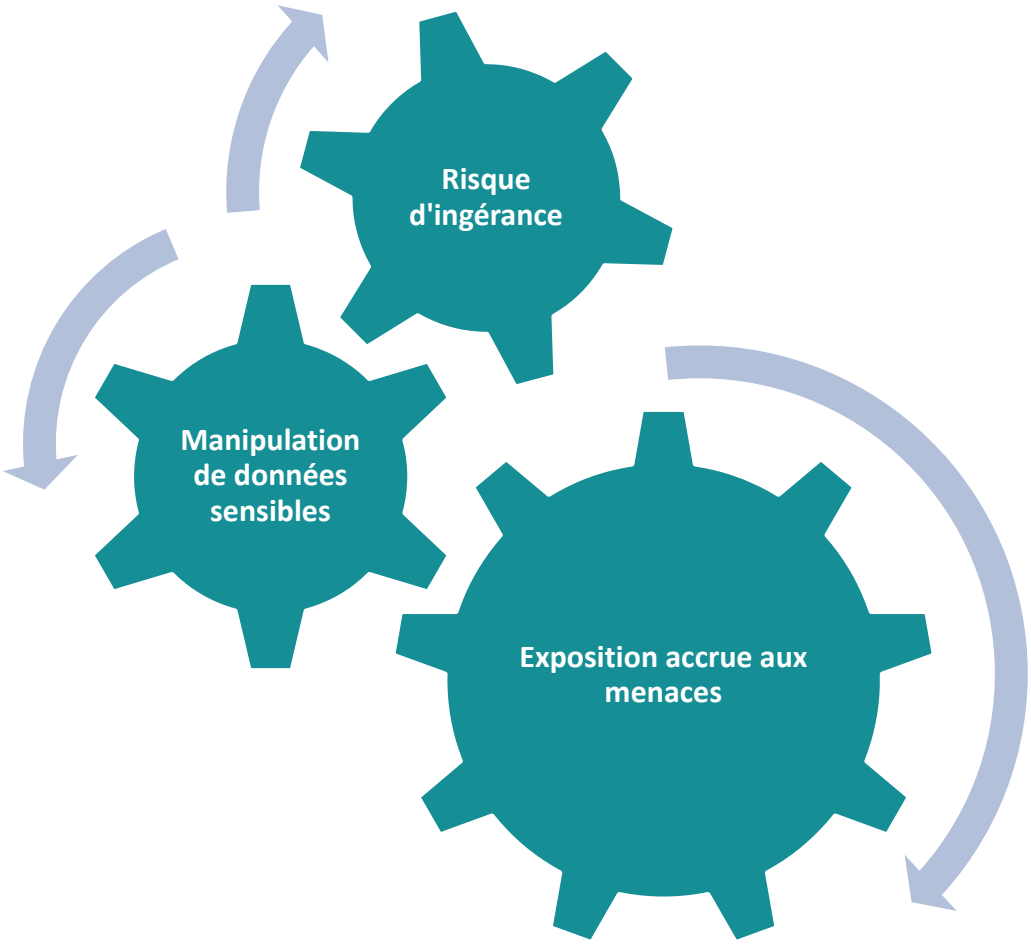
Définitions

Le tableau ci-dessous définit les termes utilisés dans la charte des administrateurs et apporte les commentaires nécessaires. Pour les autres définitions, il est renvoyé aux définitions de la charte générale.

Terme utilisé	Définition	Commentaires
Administrateur	Personnel ou prestataire qui gère en marche courante des ressources numériques dans le cadre des missions de l'établissement, en disposant du plus haut niveau d'autorisations sur le ou les systèmes qu'il administre.	Il se différencie de l'administrateur fonctionnel qui lui intervient sur les applications à travers les écrans de gestion.

Risques et opportunités

Compte-tenu du fait qu'il détient les autorisations les plus étendues sur les systèmes qu'il administre, l'administrateur technique est exposé à un niveau de risque plus élevé qu'un usager ordinaire. Certains de ces risques peuvent enrayer le bon fonctionnement des ressources numériques de l'Université Clermont Auvergne. Le schéma ci-dessous met en relief certains risques auxquels font face les administrateurs techniques.



Liste non exhaustive donnée à titre indicative

Chacun de ces risques peut engager la responsabilité de l'établissement et la responsabilité de l'administrateur concerné.

Le respect de la charte générale par les usagers et de la présente charte par les administrateurs permettront à chacun de se prémunir correctement contre les risques énoncés ci-dessus.

Application de la charte des administrateurs techniques

La présente charte s'applique exclusivement aux administrateurs techniques. Elle pourra être complétée ou amendée selon l'évolution de la Politique de Sécurité des Systèmes d'Information (PSSI) de l'établissement ou des règles d'usage des ressources numériques.

2. Droits et devoirs de l'administrateur

Droits de l'administrateur

L'établissement reconnaît des droits étendus à ses administrateurs pour les besoins de leur mission. Cette mission requiert avant tout une technicité informatique adaptée sur le périmètre confié. Elle s'opère sous la responsabilité de la DSI ou du responsable de la structure, en fonction du rattachement hiérarchique ou fonctionnel à la DSI suivant l'organigramme en vigueur. L'Administrateur bénéficie des droits spécifiques suivants :

- accès privilégié à la formation pour ce qui concerne le cadre législatif dans lequel il officie, sollicitation des services de l'établissement spécialisés dans les affaires juridiques lorsque nécessaire ;

- accéder à l'ensemble de l'infrastructure informatique du périmètre dont il a la responsabilité ;

- administrer, dans le cadre de sa mission et dans le strict respect de la confidentialité tous types de données y compris :
  -les données à caractère personnel ;
  -les données des enregistrements légaux.
  Dans ces deux cas la confidentialité est à assurer même vis-à-vis de la hiérarchie et des pairs (hors hiérarchie fonctionnelle de la sécurité des systèmes d'information)

- utiliser les moyens mis à sa disposition pour détecter toute anomalie ou incident de sécurité affectant le système informatique ;

- effectuer tout traitement (détection, analyse, éradication, filtrage, etc.) de flux informatiques présentant des risques de sécurité ;

- prendre en main à distance tout poste, selon les procédures adaptées. Il s'assure que l'utilisateur en soit informé, hors cas de menace à l'intégrité ou à la sécurité du système, ou de violation grave de la charte générale;

- modifier les autorisations accordées aux utilisateurs, sans information préalable dès lors que l'intégrité du système est mise en péril ;

- altérer les données utilisateurs, y compris personnelles, lorsque celles-ci représentent une menace potentielle et immédiate pour l'intégrité du système, en prenant des mesures conservatoires (copie sur support isolé) dès lors que possible ;

- droit de réserve :
    - *se positionner formellement quant à la conformité légale des actions demandées par l'établissement, impliquer sa hiérarchie et refuser d'agir en l'absence de trace écrite formalisant clairement la demande et dégageant sa responsabilité juridique ;*
    - *en dehors des opérations courantes et de la gestion des systèmes courants, l'administrateur peut demander à sa hiérarchie l'intervention de fournisseurs pour réaliser des tâches nécessitant une expertise plus spécifique, à défaut se déclarer non compétent à mener les actions nécessaires ;*

- mettre en place (ou obtenir la mise en place), si nécessaire, de tout système qualifié avec sa hiérarchie et ses pairs, homologué si besoin par le responsable de la sécurité des systèmes d'information, pour :
    - *maintenir les ressources en conditions de fonctionnement ;*
    - *contrôler le respect des chartes relatives au numérique ;*
    - *opérer sa mission dans un cadre sécurisé, incluant les moyens de connexions à distance, ainsi que la fourniture de matériels nomades et de différentes technologies de matériels représentatifs de ceux utilisés par les usagers.*

Devoirs de l'administrateur

L'administrateur en regard de ses droits étendus prend des engagements spécifiques vis-à-vis de l'établissement, de sa hiérarchie et du responsable de la sécurité des systèmes d'information. Il a les devoirs spécifiques suivants :

- placer son action dans le respect du cadre légal et réglementaire, s'informer de celui-ci auprès de l'établissement et connaître les références juridiques disponibles dans les chartes relatives au numérique ;

- garantir la transparence des actions d'administration et d'accès aux journaux d'enregistrements (logs) vis-à-vis du RSSI ;

- Tant que la durée de rétention légale n'a pas expirée, ne jamais altérer ou supprimer des contenus dans les journaux d'évènements (logs), quelles que soient les circonstances. Une telle action, strictement interdite, engage la responsabilité de l'agent ;

- traiter en première priorité tout incident grave ou potentiellement grave, particulièrement ceux relatifs à la sécurité des systèmes, répondre aux sollicitations du responsable de la sécurité des systèmes d'information ;

- informer en premier lieu les responsables de la sécurité des systèmes d'information de tout incident de sécurité qu'il constate et des actions correctives à mener en concertation avec eux. Ces derniers informeront l'échelon hiérarchique;

- en respectant les précautions d'usage liées aux besoins de toute enquête de sécurité, notamment la confidentialité y compris à l'égard des personnes concernées, informer les usagers qui ont été personnellement victimes d'un incident de sécurité, et les sensibiliser à la sécurité des systèmes d'information lorsqu'il s'agit de personnels de l'établissement ;

- surveiller les systèmes et informer sa hiérarchie de toute nécessité d'évolution matérielle ou logicielle nécessaire au maintien en fonctionnement dans des conditions optimales de ces ressources (dans la mesure où l'agent a accès en temps voulu à toute l'information nécessaire pour ce faire) ;

- respecter strictement la confidentialité, le caractère personnel et privé des données accédées, y compris vis-à-vis de sa hiérarchie et de ses pairs, dès lorsqu'elles ne constituent pas une menace sérieuse pour l'intégrité des systèmes ou des personnes ou une violation grave de la charte générale ;

- n'effectuer des accès aux contenus identifiés comme « strictement personnels » que dans les trois cas de figure suivant :

    - lancement d'outils automatisés pour la surveillance et l'optimisation des ressources ;
    - administration courante en présence de l'utilisateur ou avec son autorisation écrite ;
    - atteinte à la sécurité ou d'événements graves justifiant une action immédiate sans possibilité d'information préalable de l'utilisateur.

- obtenir l'accord écrit ou verbal de l'usager avant toute intervention à distance opérée manuellement sur son poste, hors les cas de menace à l'intégrité ou à la sécurité des systèmes, ou de violation grave de la charte générale ;

- opérer toute action formulée par un officier de police judiciaire et s'inscrivant dans le cadre d'une réquisition judiciaire ou administrative après avoir obtenu l'accord de l'Autorité Qualifiée de la SSI (le Président de l'université) via le RSSI ; Dans le cadre d'un problème de sécurité informatique ne communiquer aucune information en dehors de la structure sans validation préalable du RSSI. Dans tous les cas le devoir de discrétion et de confidentialité s'impose ;

- placer sous son autorité tout fournisseur contribuant à la mission d'administrateur technique et l'impliquer dans le respect de la charte ;

- garantir à sa hiérarchie un accès permanent aux systèmes qu'il administre (hors logs) pour le compte de celle-ci et ne pas faire entrave à cet accès, sous réserve du respect de la charte générale et de la présente charte par la hiérarchie;

- sous réserve de son devoir de confidentialité, expliquer à tout usager qui en fait la demande l'étendue de sa mission et les informations auxquelles il a accès ;

- être particulièrement vigilant dans l'application des règles de sécurité, en pleine conscience des autorisations étendues dont il bénéficie, et notamment pour ce qui concerne :
    - *l'accès aux systèmes via ses autorisations administrateur ;*
    - *la protection de ses propres autorisations*
    - *la remise de toute autorisation à un usager, en respectant les procédures définies par l'autorité fonctionnelle du système. Il prend toutes précautions nécessaires relatives à l'identité de l'usager ;*

En outre, l'administrateur technique observe strictement les règles de sécurité et les limites fixées à son intervention :

- il n'abuse pas de ses privilèges, et limite ses actions aux ressources informatiques dont il a la charge selon ses attributions propres ;

- il ne prend pas ses consignes auprès d'une personne non identifiée ou n'appartenant pas à l'établissement ;

- il vérifie la teneur et l'authenticité, auprès de sa hiérarchie, des instructions reçues lorsque celles-ci lui demandent d'opérer des actions susceptibles de sortir de ses missions habituelles ;
- il ne contourne pas les procédures de sécurité établies et en particulier ne désactive pas de sa propre initiative les mécanismes de traçabilité ou de filtrage mis en œuvre dans le cadre de la Politique de Sécurité des Systèmes d'Information ou dans le cadre légal.

Il effectue une copie préalable système qu'il manipule, lorsque les données de celui-ci ont une probabilité importante d'être requise ultérieurement par un officier judiciaire.

Enfin, plus généralement, l'administrateur prend les précautions suivantes :

- il respecte les engagements de confidentialité et de non-divulgation ;
- il informe le Responsable de la Sécurité des Systèmes d'Information (RSSI) de toute faille ou incident de sécurité qu'il pourrait découvrir ou dont il pourrait avoir connaissance ; Le RSSI prendra les mesures nécessaires vis-à-vis de la hiérarchie de l'administrateur.
- il préserve, conserve et sauvegarde les traces nécessaires à la résolution des incidents et à toutes investigations ultérieures, y compris judiciaires, dans des conditions permettant de garantir la valeur probante des traces ; il conserve l'information exacte de la procédure qu'il suit, ainsi que leur justification, et se coordonne avec le RSSI (notamment avant d'appliquer des corrections qui pourraient compromettre des traces).
- il n'utilise les comptes avec des droits privilégiés que pour les activités et besoins directement liés aux tâches qui lui sont confiées.

3. Les textes de référence :

Principaux textes législatifs se rapportant à la sécurité des systèmes d'information et à la protection des personnes :

- articles référencées dans la charte générale
- article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique : altération de données portant atteinte au code de la propriété intellectuelle
- article 226-13 du code pénal : respect de la confidentialité
- art. 226-16 à 24 : protection des données à caractère personnel.
- Art.28 du code de la fonction publique du 13 juillet 1983

4. Exemples de pratiques contrevenant à la charte

L'utilisation par les administrateurs des ressources numériques qui sont mises à leur disposition par l'établissement, doit être conforme à la réglementation en vigueur. Sans viser l'exhaustivité, ce chapitre illustre quelques situations propres au contexte universitaire qui contreviennent à la présente charte. Par exemple lorsqu'un administrateur :

- Donne accès à un usager aux répertoires / données personnelles d'un collègue
- Ne se déconnecte pas systématiquement des services auxquels il s'est connecté
- Fournit un listing de personnels à un collègue ou service partenaire, sans se préoccuper d'obtenir un accord écrit de l'autorité concernée
- N'informe pas le RSSI d'une situation hors du cadre légal, dès lors qu'elle est portée à sa connaissance.

5. Diffusion et révision de la charte

L'établissement révisera dès lors que nécessaire la présente charte des administrateurs techniques. Il s'engage à informer l'ensemble des usagers et à maintenir à sa disposition toute révision de celle-ci en la diffusant sur les portails intranet.

UNIVERSITE CLERMONT AUVERGNE

Politique de gestion des journaux informatiques

JANVIER 2018

1 Définitions

Dans la suite de ce document, on entend:

- Par « Système d'Information (SI) », du point de vue technique, l'ensemble des ressources participant à la gestion, au traitement, à la sécurisation, au stockage, au transport et à la diffusion de l'information au sein de notre Université.
- Par « SSI » la Sécurité des Systèmes d'Information.
- Par « RSSI » le Responsable du management de la SSI
- Par « Utilisateurs » les personnels, étudiants, hébergés, stagiaires, personnes invitées et en règle générale toute personne utilisant les moyens des systèmes d'information.
- Par « entités » les composantes, services et laboratoires.
- Par « journaux informatiques » les ressources contenant les informations qui permettent de savoir qui ou quoi accède à quelle ressource informatique et à quel moment.

2 Contexte

Les Systèmes d'Information (SI) et les données qu'ils traitent sont la garantie d'un fonctionnement performant et contribuent à la diffusion de l'image de marque de notre université. Une grande partie du patrimoine scientifique ainsi que des données à caractère personnel que nous traitons repose sur le SI.
Toutefois, les Systèmes d'Information sont des outils fragiles et leur usage s'inscrit dans un cadre réglementaire bien précis qui engage la responsabilité personnelle des utilisateurs et dans certains cas celle de l'établissement.
Le présent document va fixer les exigences à respecter et les mesures à mettre en œuvre pour une gestion appropriée des journaux informatiques.
Le responsable du traitement est le Président de l'Université représenté par le Responsable de la Sécurité des Systèmes d'Information (RSSI, rssi@uca.fr) ainsi que le Correspondant Informatique et Liberté (CIL, cil@uca.fr) ou le Délégué à la Protection des Données (DPD, dpd@uca.fr).
La finalité poursuivie est l'archivage d'informations à des fins d'historique, de défense de droit en justice, et éventuellement statistiques.
La durée de stockage est de trois mois en consultation et d'un an en archivage pour la justice.
Les destinataires sont le RSSI, les représentants SSI et éventuellement des auxiliaires de justice.
Toute procédure doit respecter l'article 39 (pour le droit d'accès) et l'article 40 (pour le droit de rectification) de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel du 6 août 2004,
Dans aucun cas il ne pourra y avoir de transfert des données à un État non membre de la Communauté Européenne sans accord préalable du CIL/DPD.

3 Les intervenants

3.1 Les utilisateurs

Tous les utilisateurs, tels qu'ils sont définis en introduction de ce document, sont tenus de respecter la politique de sécurité et les chartes en vigueur dans l'établissement.

3.2 La chaîne fonctionnelle SSI

La chaîne fonctionnelle SSI est composée des acteurs suivants :

3.2.1 Les acteurs du pilotage de la SSI

- Le Haut Fonctionnaire Sécurité de Défense et de Sécurité (HFDS) au ministère et, dans certains cas, l'Agence Nationale de la SSI (ANSSI).
- L'Autorité Qualifiée de Sécurité des Systèmes d'Information (AQSSI) qui est le Président de l'Université.
- Le Vice-Président TIC (Technologie de l'Information et de la Communication) pour assister l'AQSSI.
- Le Responsable de la Sécurité des Systèmes d'Information (RSSI) et ses suppléants.
- Le Correspondant Informatique et Libertés (CIL) ou le Délégué à la Protection des Données (DPD) pour les questions touchant aux données à caractère personnel.
- Les Chargés de la Sécurité des Systèmes d'Information (CSSI), désignés auprès du RSSI et de l'AQSSI par les responsables de structure.

Au niveau de l'établissement, un Comité spécifique pilote la Sécurité du Système d'Information. Il s'agit du CPSSI (Comité de Pilotage de la SSI). Il est composé de l'AQSSI, du VP Numérique, du DGS, du FSD, des RSSI suppléants et titulaires, du DSI et du CIL/DPD.

3.2.2 Les administrateurs systèmes et réseau

Ils ont la responsabilité opérationnelle des SI. Ils sont chargés de la mise en œuvre et de la surveillance générale des systèmes et du réseau. Ils veillent au respect des règles de sécurité des systèmes d'information. À ce titre, ils gèrent les journaux dans le respect des obligations générales de leur fonction (politique de sécurité et de confidentialité, chartes). Ils rapportent, à leur supérieur dans la chaîne fonctionnelle SSI (c'est-à-dire le RSSI qui retransmet selon la gravité), toute anomalie de fonctionnement ou tout incident pouvant laisser supposer une intrusion ou une tentative d'intrusion sur les systèmes ou le réseau.
Ils exécutent des traitements et fournissent des informations pouvant inclure des données à caractère personnel uniquement à la demande et à destination de la chaîne fonctionnelle de sécurité.

4 Principes de conservation et d’accès

4.1 Finalités des traitements

Les traitements des journaux informatiques ont pour finalités :
• d'être à même de fournir les éléments de preuves nécessaires pour mener les enquêtes en cas d’incident, ainsi que de répondre à toute réquisition de l’autorité judiciaire présentée dans les formes légales ;
• de vérifier, à postériori, que les règles en matière de sécurité des systèmes d’information (SSI) sont correctement appliquées ;
• de détecter toute défaillance ou anomalie de sécurité, volontaire ou accidentelle, passive ou active, d’origine matérielle ou humaine ;
• de détecter toute violation de la loi ou tout abus d’utilisation des moyens informatiques pouvant engager la responsabilité de l’établissement ;
• de détecter les utilisations des moyens informatiques contraires aux chartes ou au règlement intérieur de l'établissement ;
• de vérifier le volume d’utilisation des ressources et de détecter des anomalies afin de mettre en place une qualité de service et de faire évoluer les équipements en fonction des besoins (métrologie).

Les finalités précitées imposent d’aller au-delà d’un enregistrement et d’une exploitation de données statistiques. Elles impliquent nécessairement l’enregistrement, la conservation temporaire et l’éventuelle exploitation de données à caractère personnel, dans la mesure où des éléments contenus dans les traces permettraient d’identifier l’utilisateur et la nature de son activité.

Ces journaux et leur traitement doivent respecter les droits de chacun et notamment être conformes à la réglementation en vigueur relative à la protection des données à caractère personnel. Ils doivent avoir satisfait au principe d’information préalable et de transparence.

4.2 Durée de conservation

La durée de conservation des journaux informatiques est de 1 an sous forme non anonymisée. L'établissement s'interdit de les exploiter sous cette forme au-delà de 3 mois sauf sur réquisition officielle ou sous une forme rendue anonyme.

Par exemple, une organisation peut être la suivante avec deux conteneurs de données définis :

- le premier reçoit les informations vieilles de moins de trois mois et les fichiers anonymisés quand ils existent (c’est-à-dire les enregistrements de plus de 3 mois qui devront être anonymisés si on souhaite les conserver sur le même conteneur).
- le second reçoit les journaux contenant des données à caractère nominatif de plus de trois mois et de moins de 1 an.

Les informations de plus de 1 an doivent être systématiquement détruites s’il n’y a pas de dispositif d’anonymisation. Des traitements statistiques peuvent cependant être opérés puis archivés comme historique et éléments de gestion de la qualité.

4.3 Qualités des données collectées

Les informations journalisées doivent être factuelles et contextuelles, c'est à dire qu'elles doivent permettre de connaître l'environnement de la collecte : le système hôte, les logiciels mis en œuvre etc. La date et l'heure sont des informations importantes parce qu'elles sont le premier élément utilisé pour rapprocher des journaux de différents serveurs. Il est donc indispensable que les machines produisant des journaux soient synchronisées sur un serveur de temps de type NTP (Network Time Protocol). Compte tenu du caractère critique de l'horodatage, les journaux NTP doivent être archivés, eux aussi, de manière sécurisée.

4.4 Sécurité et intégrité des données

L'intégrité des données doit être assurée en protégeant les journaux en particulier contre un effacement ou des modifications malveillantes.
Les règles de sécurité limitent l'accès aux journaux, en lecture seule, aux administrateurs destinataires de ces données tels qu'ils sont définis au paragraphe 3.2.2 avec authentification préalable, ainsi qu'au RSSI et aux personnes désignées par lui. Les accès sont ponctuels et motivés par les tâches de ces personnels.
Ces tâches sont réalisées dans le cadre :

- soit de l'exploitation au quotidien pour les vérifications d'usage ou l'optimisation des ressources.
- soit d'une demande de consultation des informations le concernant de la part d'un utilisateur.
- soit d'une requête de l'autorité judiciaire, requête impérativement portée à la connaissance et validée par l'AQSSI et par le service juridique de l'UCA.

Les journaux contenant des données à caractère personnel sont identifiés et référencés dans le but de garantir leur suppression au-delà d'une année.
Dans le cas d'une exploitation des journaux informatiques anonymisés, la procédure d'anonymisation est réalisée dans le respect des règles de l'art et elle est irréversible. On se référera en particulier à l'expertise publiée par la CNIL dans ce domaine (cf le guide « La sécurité des données personnelles », fiche n°16 – « l'Anonymisation »)

5 Les informations enregistrées

5.1 Informations journalisées par les serveurs (hors messagerie et Web)

Pour chaque tentative de connexion, d'ouverture de session de travail ou de demande d'augmentation de ses droits, les informations suivantes seront enregistrées automatiquement par les mécanismes de journalisation du service :

- l'identité de l'émetteur de la requête ;
- la date et l'heure de la tentative ;
- le résultat de la tentative (succès ou échec) ;
- les commandes passées ;
- les services utilisés.

Le choix d'une politique de centralisation des journaux informatiques des postes de travail peut être fait au niveau d'une composante ou d'une organisation locale.

5.2 Les équipements réseau

On appelle « équipements réseau » les routeurs, pare-feu, commutateurs, bornes d'accès, équipement de métrologie et d'administration de réseau, etc. Pour chaque paquet qui traverse l'équipement, tout ou partie des informations suivantes peuvent être collectées :
• les noms ou adresses IP source et destination ;
• les numéros de port source et destination ainsi que le protocole de transport (UDP ou TCP);
• la date et l'heure de la tentative ;
• la façon dont le paquet a été traité par l'équipement ;
• le nombre de paquets et le nombre d'octets transférés ;
• les données d'authentification ;
• les messages d'alerte.

5.3 Services de messagerie, de messagerie instantanée, de forum et de listes de diffusion

Les serveurs hébergeant ces services mis en œuvre au sein de l'établissement enregistrent pour chaque message émis ou reçu tout ou partie des informations suivantes :
• l'adresse de l'expéditeur et éventuellement des éléments identifiant celui qui s'est connecté au serveur ;
• l'adresse des destinataires ;
• la date et l'heure de la tentative ;
• les différentes machines traversées par le message dans la mesure du possible ;
• le traitement « accepté ou rejeté » du message ;
• la taille du message ;
• certaines en-têtes du message, tel que l'identifiant numérique de message ;
• le résultat du traitement des courriers non sollicités (spam) ;
• le résultat du traitement antiviral.

Les éléments de contenu des messages ne sont pas journalisés. Néanmoins, les applications peuvent inclure des archives qui ne relèvent pas des journaux informatiques (chrono départ et réception).

5.4 Serveurs Web

On distingue les serveurs web exploités au sein de l'établissement et ceux situés en dehors de l'établissement.

5.4.1 Serveurs Web de l'établissement

Pour chaque connexion, les serveurs Web enregistrent tout ou partie des informations suivantes, en fonction des exigences de qualité de service et de sécurité de l'application web :
• les noms ou adresses IP source et destination ;
• les différentes données d'authentification dans le cas d'un accès authentifié (intranet par exemple) ;
• l'URL de la page consultée et les informations fournies par le client ;
• le type de la requête ;
• la date et l'heure de la tentative ;
• le volume de données transférées ;
• les différents paramètres passés, dans la mesure du possible.

5.4.2 Serveurs Web hors établissement

Lorsque les utilisateurs sont des membres de l'établissement, pour chaque accès web via le réseau interne vers des serveurs externes, sont enregistrées tout ou partie des informations suivantes :
• les noms ou adresses IP source et destination et les différentes données d'authentification ;
• l'URL de la page consultée ;
• le type de la requête ;
• la date et l'heure de la tentative ;
• le volume de données transférées.

Lorsque l'établissement offre des accès internet à des personnes extérieures, il est alors possible d'assimiler le service réseau de l'établissement à celui d'un opérateur de communications électroniques.
Dans ce cas, l'enregistrement se fait dans le cadre de l'article L.34-1 du code des postes et des communications électroniques. Il est précisé que les opérateurs de communications électroniques sont tenus à une obligation de conservation des données de connexion mais que celles-ci "ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications". Cette interdiction s'applique donc en particulier à l'URL des pages consultées.

5.5 La téléphonie sur IP

L'usage de la téléphonie sur IP peut engendrer des enjeux spécifiques dans le domaine de la sécurité ou dans celui du contrôle du bon fonctionnement des réseaux, mais bien entendu, les principes relatifs à la loi « Informatique et Libertés » s'appliquent à la téléphonie sur IP comme aux autres systèmes de téléphonie.
Lorsque des relevés justificatifs des numéros de téléphone appelés sont établis, les quatre derniers chiffres de ces numéros sont occultés. Cependant, l'établissement peut éditer des relevés contenant l'intégralité des numéros appelés dans le cas où il demande aux personnels le remboursement du coût des communications personnelles, ou dans celui où il a été constaté une utilisation manifestement anormale.
Le régime déclaratif de ces journaux fait l'objet de la norme simplifiée n° 47 de la CNIL (NS-047 n°2005-019 du 03/02/2005) relative à l'utilisation de services de téléphonie fixe ou mobile sur les lieux de travail.
En outre, la fiche pratique CNIL n°11 du guide « informatique et libertés » pour l'enseignement supérieur et la recherche, intitulée « Utilisation du téléphone sur le lieu de travail », détaille ce cas.

5.6 Les applications spécifiques

On entend par «applications spécifiques», toute application autre que celles mentionnées ci-dessus et qui nécessite pour des raisons de comptabilité, de gestion, de sécurité ou de développement, l'enregistrement de certains paramètres de connexion et d'utilisation.

Parmi ces applications nous pouvons citer les exemples suivants :

- accès aux bases de données ;
- accès à l'ENT (espace numérique de travail) ;
- service d'authentification (SSO, radius, …) ;
- …

De manière générale, des journaux génériques sont susceptibles d'être constitués et tout ou partie des informations suivantes peuvent être collectées :

- l'identité de l'émetteur de la requête ;
- les noms ou adresse IP source ;
- la date et l'heure de la tentative ;
- le résultat de la tentative ;
- les volumes de données transférées ;
- les commandes passées ;
- les traitements demandés.

Le traitement des journaux, décrit ici, ne couvre pas l'ensemble des données conservées par ces applications, qui de par leur nature, peuvent historiser certaines transactions. Il est rappelé que si ces données visant à assurer la traçabilité des opérations ont un caractère personnel, elles sont alors soumises aux obligations réglementaires et doivent faire l'objet de toute déclaration nécessaire auprès du CIL/DPD, avec une information préalable des utilisateurs.

6 Finalités des traitements effectués et leurs destinataires

Les traitements effectués doivent permettre d'obtenir des journaux qui répondent aux principes énoncés précédemment, tout en restant conformes aux obligations légales sur la protection des données à caractère personnel et de la vie privée. Ils doivent faire l'objet de toute déclaration légale nécessaire auprès du CIL/DPD.

6.1 Résultats statistiques

Ceux-ci sont obtenus automatiquement et permettent de contrôler les volumes d'utilisation des moyens mis à la disposition des utilisateurs en tant qu'outil de travail. Lors de l'exploitation de ces résultats, on s'attachera à distinguer les résultats anonymes de ceux qui peuvent être rapprochés de l'identité d'une personne. Parmi tous ces traitements on trouvera :
• des traitements statistiques anonymes, en volume transféré et en nombre de connexions ;
• des classements des services les plus utilisés en volume de données et en nombre de connexions.
Les résultats « anonymes » peuvent être conservés au-delà des délais mentionnés au paragraphe 3 et être diffusés sur des sites Internet accessibles à tous. Par contre, les administrateurs systèmes et réseau limitent l'accès aux résultats contenant des données à caractère personnel à eux-mêmes et au RSSI. La durée de conservation de ces statistiques non anonymisées ne peut excéder celle des journaux utilisés pour produire ces statistiques.
Dans tous les cas, les administrateurs ne devront divulguer aucun élément personnel dont ils auraient connaissance et qui ne serait pas utile à la finalité de ce traitement.

6.2 Résultats d'analyse

La politique de sécurité, applicable à chaque ressource informatique qui génère des traces, définit des règles d'analyse systématique de ces traces afin de pouvoir détecter, dans les meilleurs délais, les incidents relatifs à la sécurité des systèmes d'information.
En cas d'incident, des analyses peuvent être faites par les administrateurs systèmes et réseau sur les traces disponibles. Les résultats ne peuvent être transmis qu'à la chaîne fonctionnelle SSI.
Dans ce cas, l'accès aux trafics et aux traces est limité au RSSI et aux exploitants des systèmes en charge d'analyser l'incident. L'extraction de l'information et son utilisation sont strictement limitées à l'analyse de l'incident. Si l'incident n'est pas avéré, les résultats ne sont pas retransmis et immédiatement détruits.

6.3 Détection des usages abusifs

On entend par « usages abusifs » les usages du réseau qui sont contraires aux lois, règlement intérieur ou chartes d'usage des moyens informatiques. Sont aussi visés les usages qui compromettent les services du réseau de l'établissement (consommation excessive de bande passante, introduction de faille dans la sécurité du réseau, etc).

Les journaux peuvent être exploités pour mettre en évidence ces abus. Par exemple, des classements des machines ayant consommé le plus de ressources réseau en volume transféré et en nombre de connexions permettent souvent de détecter l'utilisation indésirable de protocoles de peer to peer ou la présence de serveurs pirates.
Quand ils sont mis en œuvre, ces traitements doivent l'être de façon systématique (ils sont appliqués à toutes les machines du réseau de l'établissement ou d'une partie donnée du réseau comme par exemple une composante ou un laboratoire) et ne doivent cibler aucune personne ou catégorie de personnes.

6.4 Journaux bruts

Ceux-ci permettent de replacer une action particulière dans son contexte, à des fins d'enquête.
Dès l'apparition d'un incident, les journaux bruts pourront être requis par la chaîne fonctionnelle.
Les administrateurs systèmes et réseau sont chargés de l'application de la requête, et ils sont, pour cette activité, soumis au secret professionnel.
Les journaux bruts sont remis immédiatement à la chaîne SSI, à sa requête.
L'AQSSI transmettra ensuite les éléments à l'autorité judiciaire afin de lui permettre de poursuivre une enquête.

6.5 Droit d'accès individuel

Chaque agent peut demander à consulter les traces qui le concernent. Les demandes doivent être faites par écrit auprès du directeur de la structure de rattachement. Celui-ci transmettra au CIL/DPD.
Après validation, la recherche sera faite par l'administrateur et les résultats seront transmis directement à l'utilisateur demandeur, sous la forme d'un «courrier personnel» avec accusé de réception. Cette communication se fera de préférence sous format papier (sauf accord de l'intéressé pour une transmission électronique).

6.6 Droits d'accès aux journaux (hors droits d'accès individuels, cf § 6.5)

En dehors des acteurs de la chaîne fonctionnelle SSI, personne (y compris la chaîne hiérarchique) n'a de droit d'accès aux journaux informatiques comportant des données à caractère personnel.
Les acteurs SSI sont tenus au devoir de réserve, à la discrétion professionnelle et au secret professionnel.

7 Informations des utilisateurs sur la politique de gestion des journaux informatiques

L'établissement doit informer ses utilisateurs de la gestion qui est faite des traces qui les concernent. Cela sera fait par la diffusion systématique de ce document qui sera référencé dans la charte informatique de l'établissement. Ce document sera rendu accessible à tout utilisateur

de manière électronique. Il pourra être mis en valeur dans l'intranet de l'établissement ou par voie d'affichage. Une attention particulière sera portée à la publicité de ce document lors de la mise à disposition de nouveaux services concernés par les journaux informatiques, ainsi qu'auprès des nouveaux utilisateurs des moyens informatiques de l'établissement.
Une information et une consultation préalable des instances représentatives des personnels doit être prévue.