

**DÉLIBÉRATION PORTANT ADOPTION DE LA CHARTE INFORMATIQUE
ET DE LA POLITIQUE GENERALE DE SECURITE DES SYSTEMES
D'INFORMATION DE L'UNIVERSITÉ DE BORDEAUX**

Vu les dispositions du code de l'éducation et notamment les articles L. 712-1 et L. 712-3 ;

Vu les statuts de l'université de Bordeaux ;

Vu l'avis de la commission des statuts du xx/xx/xx ;

Vu l'avis du comité social d'administration de l'université de Bordeaux du 12 mai 2023 ;

Le conseil d'administration, après en avoir délibéré, décide :

Article 1.

La charte informatique et la politique générale de sécurité des systèmes d'information de l'université de Bordeaux, joints à la présente délibération, sont adoptés.

Article 2.

La présente délibération sera transmise au recteur de région académique Nouvelle-Aquitaine. Elle sera publiée conformément aux dispositions relatives à la publication des actes à caractère réglementaire de l'université de Bordeaux.

Le président du conseil d'administration,

Dean LEWIS

Président de l'université de Bordeaux

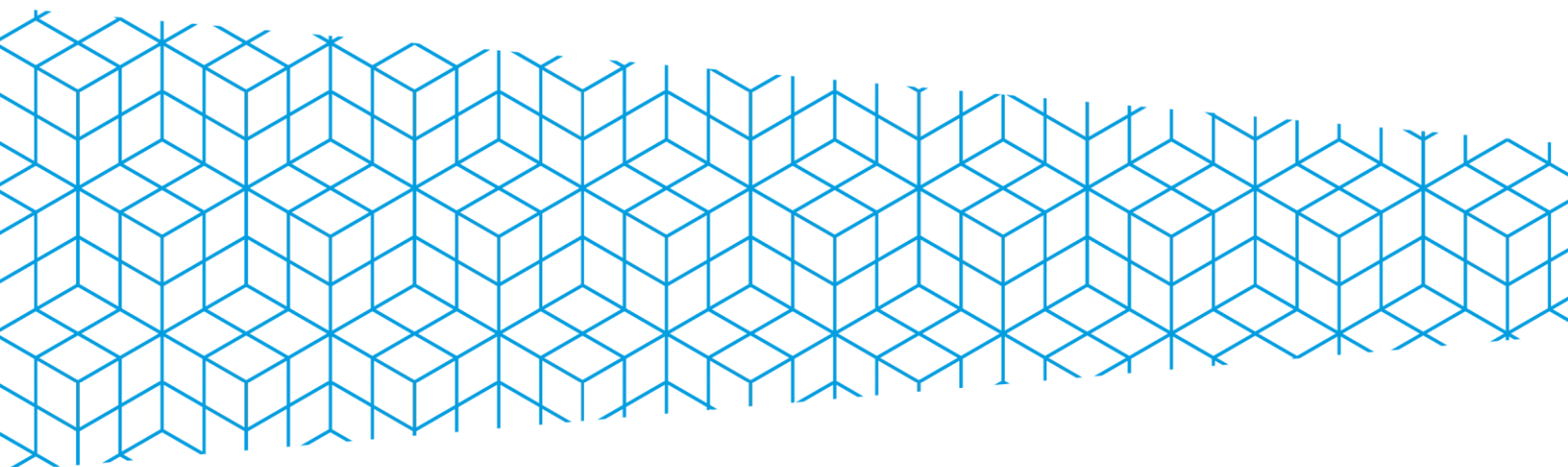
Adoptée à la majorité des
votes exprimés (29 votants)
Pour : 29
Contre : 0
Abstention : 0



POLITIQUE GENERALE DE SECURITE DES SYSTEMES D'INFORMATION

Version : 1.0

Date de publication : 30/05/2023



Rédaction

Soben CHHEM (RSSI)

Jean-Marc COUVEIGNES
(Chargé de mission sécurité)

Principaux contributeurs :

Karim BELEBAS (VP Numérique)

Frédéric POMIES (Directeur des Systèmes d'Information)

Table des matières

Lettre d'engagement de la Présidence.....	3
I. Définition.....	5
II. Introduction	6
II.1 Objectif	6
II.2 Fondements juridiques.....	6
II.3 Périmètre d'application	6
II.4 Corpus documentaire SSI.....	7
III. Organisation et gouvernance de la SSI	8
III.1 Rôles et responsabilités	8
III.1.1 L'AQSSI.....	8
III.1.2 Le VP Numérique	9
III.1.3 Le Chargé de mission SSI.....	9
III.1.4 Le RSSI	9
III.1.5 Le DSI.....	10
III.1.6 Le Fonctionnaire Sécurité et Défense (FSD)	10
III.1.7 Le correspondant SSI.....	10
III.2 Instances de gouvernance de la sécurité	11
III.2.1 Le Comité stratégique de la sécurité des SI	11
III.2.2 Le Comité de pilotage de la sécurité des SI.....	12
III.2.3 Le Comité de suivi de la sécurité des SI	12
IV. Principes de mise en œuvre	13
IV.1 Garantir la sécurité des SI	13
IV.2 Identifier les risques et définir les mesures prioritaires.....	13
IV.3 Intégrer la sécurité dans les projets	14
IV.4 Gérer les incidents SSI	15
IV.5 Contrôler et assurer la conformité.....	15
IV.5.1 Cadre réglementaire et conformité.....	15
IV.5.2 Audits internes.....	16
IV.5.3 Réévaluer la PGSSI	17

Lettre d'engagement de la Présidence

Par cette politique générale de sécurité des systèmes d'information (**PGSSI**), la Présidence de l'université de Bordeaux, consciente de l'accroissement et de la diversification des risques, et de l'importance cruciale de la cybersécurité pour la continuité et la qualité de ses activités, souhaite réaffirmer son engagement total en la matière.

L'université de Bordeaux est une grande institution française reconnue en Aquitaine, sur le territoire national et dans le monde, pour l'excellence de ses formations, la qualité de sa recherche, l'intensité et la diversité de son activité d'innovation et de diffusion.

Afin de mieux répondre aux défis scientifiques, aux attentes sociétales et aux urgences environnementales, l'université de Bordeaux s'affirme comme **université étendue**, connectée, ancrée dans ses territoires, ouverte à la société et à la diversité, innovante et intensive en recherche.

Pour réussir cette transformation, l'université de Bordeaux entretient et développe de **nombreux partenariats** scientifiques, institutionnels, territoriaux, culturels.

Vecteur de connaissances, de progrès social et sociétal, d'ouverture, de performance et de rationalisation, la **transition numérique** est au cœur du projet de l'Université. Elle est un instrument majeur de l'innovation pédagogique, de la recherche scientifique, de la qualité de vie sur le campus, de l'efficacité administrative et énergétique, de l'information et de la documentation scientifiques, de la visibilité et de l'attractivité de l'Université.

Le succès de cette transition numérique conditionne donc la réussite du projet de l'Université.

Parce que la **confiance** dans les systèmes d'information est indispensable à la transition numérique, la **cybersécurité** est un **enjeu majeur** de cette transition.

L'Université doit en effet garantir la résilience et l'interopérabilité de ses systèmes d'information. Elle doit protéger son patrimoine informationnel et les utilisateurs de ses systèmes d'information. Elle doit se conformer aux exigences légales et réglementaires et respecter ses engagements contractuels en matière de sécurité.

Pour y parvenir l'Université informe et mobilise **l'ensemble de la communauté académique** (personnels, usagers, partenaires) sur les enjeux, les règles et les bonnes pratiques de la cybersécurité, la prévention et la gestion des risques.

Elle met en place une organisation et une gouvernance de la sécurité des systèmes d'information qui sont décrites dans la politique générale de sécurité des systèmes d'information.

Cette politique générale de sécurité des systèmes d'information de l'université de Bordeaux fournit **un cadre de référence** et de cohérence à la sécurité des systèmes d'information. Elle définit les principes généraux de sécurité à respecter, ainsi que **l'organisation et les responsabilités en matière de sécurité des SI**. Comme l'ensemble des politiques et directives de sécurité, elle s'applique à toutes les structures de l'Université et à tous les utilisateurs de ses systèmes d'information.

Sous la coordination du Responsable de la sécurité des systèmes d'information, plusieurs axes majeurs sont à prendre en compte :

- Renforcer la confiance numérique pour améliorer l'attractivité de l'Université
- Faire évoluer le modèle de gouvernance et de pilotage de la sécurité intégrant les partenaires et les tiers
- Être un acteur de la conformité et assurer la protection de l'information
- Assurer un niveau de résilience élevé pour l'ensemble des activités

L'engagement de l'université de Bordeaux pour la cybersécurité s'inscrit dans une démarche de qualité du service public, d'excellence et de rayonnement scientifique, de progrès sociétal et environnemental, d'efficacité, de conformité réglementaire.

Cet engagement est celui de toute la communauté universitaire.

Le Président

Le 06, 01, 22

A handwritten signature in blue ink, consisting of a large, stylized initial 'L' followed by a smaller 'P' and a long horizontal stroke extending to the right.

I. Définition

Analyse de risques	Processus visant à identifier les risques, déterminer leurs impacts et leur probabilité d'occurrence et définir les mesures de sécurité nécessaires
Audit	Opération visant à analyser les actions effectuées sur des données ou des biens ou à mesurer l'écart par rapport à un référentiel (par exemple la PSSI-E) ou par rapport à l'état de l'art.
Autorité Qualifiée pour la sécurité des systèmes d'Information (AQSSI)	Autorité juridiquement responsable de la sécurité des systèmes d'information de l'université de Bordeaux. Sa responsabilité ne peut être déléguée
Partie prenante	Personne ou organisme susceptible d'affecter, d'être affecté ou de se sentir lui-même affecté par une décision ou une activité
Plan d'assurance sécurité (PAS)	Ensemble des dispositions que le prestataire prendra pour garantir le respect des exigences de sécurité du bénéficiaire.
Protection du potentiel scientifique et technique de la nation (PPST)	Dispositif protection contre l'espionnage technologique visant à protéger, au sein des établissements publics et privés, les savoirs et savoir-faire stratégiques ainsi que les technologies sensibles qu'ils détiennent.
Politique de sécurité du système d'information (PSSI)	Ensemble de règles et d'exigences permettant d'assurer un niveau de sécurité conforme aux besoins de l'Université et permettant d'assurer une conformité réglementaire
Sécurité des systèmes d'information (SSI)	Ensemble des moyens techniques, organisationnels, juridiques et humains nécessaire à la protection des systèmes d'information contre les accidents (pannes, pertes, événements etc.), les erreurs (d'utilisation, de conception) et les actes malveillants (piratage, vol, captation d'information, ingénierie sociale, etc.).
Système d'information (SI)	Ensemble d'applications, services, actifs informationnels ou autres composants permettant de gérer l'information.

II. Introduction

II.1 Objectif

La Politique Générale de Sécurité du Système d'Information (**PGSSI**), a pour objectif de fournir un cadre de référence et de cohérence en matière de sécurité des systèmes d'information de l'université de Bordeaux. C'est un document fondateur qui s'inscrit dans un ensemble plus large de documents décrivant les exigences et règles de sécurité attendues afin d'assurer la protection des SI et la conformité réglementaire sur l'ensemble de ses activités, de ses projets vis-à-vis de ses partenaires, ses campus distants et ses annexes.

Elle définit les principes généraux de sécurité, le périmètre ainsi que l'organisation et les responsabilités en matière de sécurité des SI afin de :

- Renforcer la confiance numérique pour améliorer l'attractivité de l'Université
- Faire évoluer le modèle de gouvernance et de pilotage de la sécurité intégrant les partenaires et les tiers
- Être un acteur de la conformité et assurer la protection de l'information
- Assurer un niveau de résilience élevé pour l'ensemble des activités

II.2 Fondements juridiques

La PGSSI s'appuie sur les règlements et les directives ministérielles suivantes :

- La Politique de Sécurité des Systèmes d'Information de l'État (PSSI-E)
- Le décret n°2022-513 du 8 avril 2022 relatif à la sécurité du système d'information et de communication de l'État et de ses établissements publics
- L'instruction générale interministérielle n°1337/SGDSN/ANSSI
- Le référentiel général de sécurité (RGS)
- Le règlement général sur la protection des données (RGPD)
- La réglementation sur l'hébergement des données de santé (HDS)
- Le code de la défense
- Le code de l'éducation, notamment l'Article L712-2

La PGSSI s'appuie également sur les recommandations de l'agence nationale de la sécurité des systèmes d'information (ANSSI).

II.3 Périmètre d'application

La PGSSI s'applique à toutes les structures de l'université de Bordeaux, à tous les utilisateurs et les constituants de ses systèmes d'information (les données, les processus, les composants techniques matériels et logiciels, les infrastructures, etc)

Par structures de l'Université on entend les composantes de l'Université mentionnées à l'Annexe 3 des statuts de l'Université, notamment les collèges, les composantes de formation,

l'IUT, l'INSPE, l'ISVV, le collège des écoles doctorales, les départements de recherche, les unités et structures de recherche, l'OASU, ... ainsi que les pôles, directions et services.

Par utilisateur on entend toute personne accédant aux moyens informatiques de l'Université, notamment et non exclusivement les personnels titulaires ou contractuels de l'Université, les étudiants, les personnels des partenaires, les bénéficiaires ou prestataires de l'Université, les visiteurs, les invités, les intervenants extérieurs, etc.

Les termes université de Bordeaux et Université seront employés indifféremment.

La direction de chacune des structures administratives, composantes de formation, laboratoires de recherche et plateformes scientifiques interagissant avec le SI de l'université de Bordeaux est responsable de l'application de la PGSSI et des politiques de sécurité sur l'ensemble de son périmètre d'activité.

D'autre part, les utilisateurs des systèmes d'information de l'Université doivent respecter la charte informatique.

Il est entendu que l'application de la PGSSI se fait dans le respect du décret n°82-447 du 28 mai 1982 relatif à l'exercice du droit syndical dans la fonction publique et de la charte de l' élu en vigueur au sein de l'établissement et de tout document qui viendrait à s'y substituer.

La PGSSI est diffusable et peut être communiquée à toute entité justifiant le besoin d'en connaître.

II.4 Corpus documentaire SSI

La politique de sécurité du système d'information de l'Université fait partie d'un référentiel documentaire à quatre niveaux :

- Le présent document, la Politique Générale, en constitue le premier niveau. Il décrit le cadre de référence en matière de sécurité du SI et fixe les enjeux et les principes de gouvernance.
- Un standard de sécurité (socle commun d'exigences de sécurité attendues) et des politiques thématiques (un ensemble de documents qui définit plus précisément les processus et règles de sécurité à mettre en œuvre par thème)
 - Politique de gestion des vulnérabilités
 - Politique de gestion des risques
 - Politique d'autorisation des exceptions
 - etc
- Des directives, à savoir les conditions, les lignes de conduite et les règles à adopter pour utiliser et gérer les services et actifs des SI de l'Université
- Des déclinaisons techniques. Il s'agit de guides, des bonnes pratiques, des procédures et des FAQ qui viennent compléter les politiques thématiques, dans des environnements techniques et organisationnels spécifiques.

La politique générale de sécurité et les politiques de sécurité thématiques de l'université de Bordeaux précisent les lignes directrices et les principes de sécurité à mettre en œuvre.

Il revient ensuite à chaque structure de décliner sa propre politique de sécurité, en se basant sur les principes et mesures de sécurité de l'Université, afin de prendre en compte les

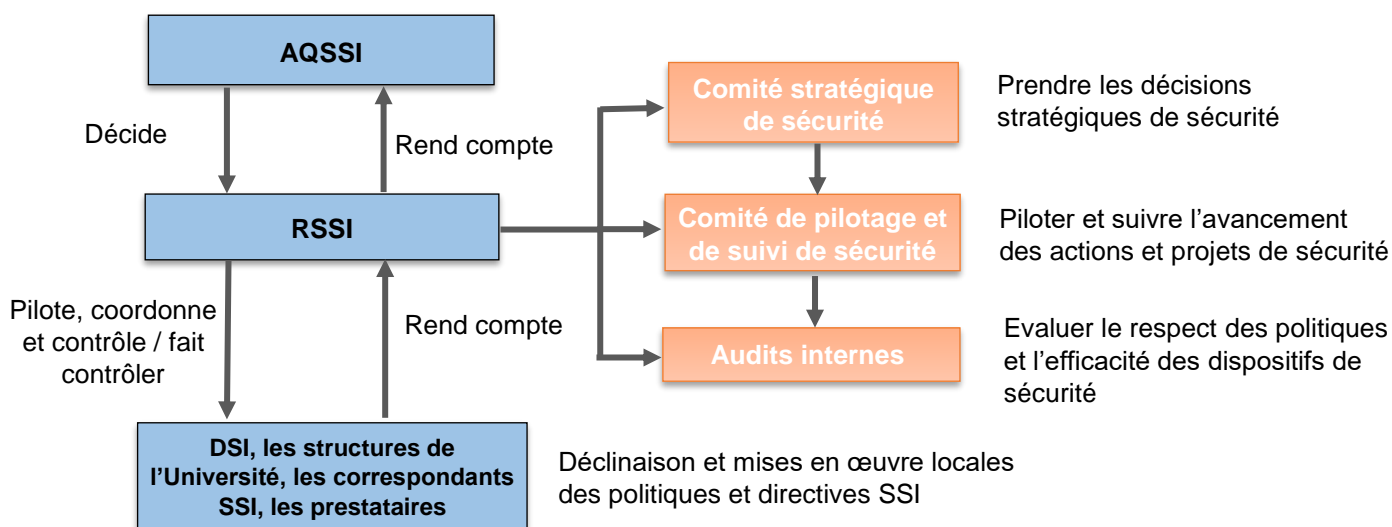
spécificités de son environnement (enjeux, menaces, besoins, réglementation sectorielle ou orientations des autres tutelles).

Chaque structure est responsable de la mise en œuvre opérationnelle.

III. Organisation et gouvernance de la SSI

La présidence de l'Université est l'autorité qualifiée en matière de SSI (AQSSI).

A travers un dispositif organisationnel dédié, elle s'appuie sur des rôles et responsabilités distribués à tous les niveaux pour coordonner l'ensemble des actions et mesures de sécurité et faciliter l'application de la PGSSI sur son périmètre.



III.1 Rôles et responsabilités

III.1.1 L'AQSSI

L'autorité qualifiée pour la sécurité du système d'information (AQSSI) est le responsable juridique de la sécurité des SI au sein de son établissement. A ce titre il est le décisionnaire de l'organisation de la SSI et des mesures de sécurité à appliquer. Le président de l'université de Bordeaux en tant que Chef d'établissement porte cette fonction.

Il a pour rôle principal :

- De définir la politique de sécurité des systèmes d'information et de fixer les objectifs en matière de sécurité des SI pour l'établissement et pour toutes les entités rattachées, ou bénéficiaires des moyens informatiques mis à disposition par la DSI de l'université de Bordeaux.
- D'assurer la responsabilité globale du niveau de sécurité nécessaire pour toutes les activités portées au sein de l'établissement
- De veiller au respect du cadre réglementaire et légal
- D'arbitrer le plan de traitement des risques et les ressources et moyens alloués

- De faire mener les contrôles et audits nécessaires au sein même des structures de l'université de Bordeaux, mais aussi chez les partenaires extérieurs et prestataires
- D'intenter des actions en justice si nécessaire

L'AQSSI nomme et mandate le RSSI pour mener toutes les actions utiles au sein de l'université de Bordeaux au regard des exigences réglementaires et de l'état de l'art en matière de SSI.

III.1.2 Le VP Numérique

Le VP numérique, entre autre missions, assure le pilotage politique de la SSI, sa mise en application au sein de l'Université et des composantes qui lui sont rattachées, et la bonne articulation et meilleure cohérence avec la protection du potentiel scientifique et technique (PPST). Il est aussi responsable de la définition et de la mise en œuvre du cadre partenarial de la SSI, notamment en lien avec les organismes nationaux de recherche avec lesquels l'Université partage la tutelle des laboratoires.

III.1.3 Le Chargé de mission SSI

Le chargé de mission SSI assiste le VP Numérique dans le portage politique de la SSI. Il est l'interlocuteur privilégié des Directeurs des structures, des composantes de formation, des laboratoires de recherche et des plateformes scientifiques dans la déclinaison et la mise en œuvre des politiques de sécurité.

Il anime le réseau des correspondants SSI et supervise la mise en œuvre des actions de sécurité, les analyses de risques, les plans d'actions préventifs et l'appropriation des enjeux SSI sur l'ensemble du cycle de vie des projets informatiques portés par chaque entité.

En matière de sécurité des SI, il représente l'équipe politique de l'Université auprès des organismes et services de l'Etat ainsi qu'auprès des partenaires de l'Université.

III.1.4 Le RSSI

Le Responsable de la Sécurité des Systèmes d'Information, rattaché hiérarchiquement à l'AQSSI, a pour mission de formaliser les politiques de sécurité des SI, d'organiser et de coordonner la mise en œuvre des politiques de sécurité. Il est force de proposition et de conseil auprès du VP Numérique, du chargé de mission, des directions, des responsables de structures et des responsables de départements.

Il s'appuie sur la DSI et les correspondants SSI de chaque structure pour la mise en œuvre des actions de sécurité, les analyses de risques, les plans d'actions préventifs et l'appropriation des enjeux de la SSI sur l'ensemble du cycle de vie des projets informatiques portés par chaque entité.

Le RSSI est l'interlocuteur opérationnel privilégié pour les organismes et services de l'état (ANSSI, DGSI, COSSIM...), les structures de l'Université, et toute entité collaborant avec l'Université ou en interaction avec elle (partenaires, prestataires, collectivités, associations, etc.).

Le RSSI est associé au pilotage des projets et définit les exigences de sécurité afin d'impulser les actions de sécurisation adaptées aux contextes, à l'état de l'art et dans le respect des exigences réglementaires.

III.1.5 Le DSI

Le Directeur des Systèmes d'Information (DSI), dirige les Systèmes d'Information de l'université de Bordeaux. Il s'appuie sur les accords de coordination établis avec les composantes, laboratoires et plateformes scientifiques pour articuler leurs systèmes d'information propres.

Le DSI, définit la stratégie en matière de mise en oeuvre de la SSI, afin de décliner les politiques et objectifs de sécurité en projets, en mesures et actions de sécurisation.

Dans cet objectif, le DSI coordonne l'action de ses équipes avec le RSSI et le DPO en vue d'intégrer les exigences de sécurité sur l'ensemble des systèmes d'information et des services associés, tout en respectant le besoin de protection des données à caractère personnel, et plus largement le patrimoine informationnel.

III.1.6 Le Fonctionnaire Sécurité et Défense (FSD)

Le Fonctionnaire de sécurité et de défense (FSD) est nommé par le Haut Fonctionnaire de défense et de sécurité (HFDS). En tant que relais fonctionnel du HFDS, le FSD est placé sous l'autorité du président de l'Université qu'il assiste pour l'exercice de ses responsabilités en matière de défense et de sécurité.

A ce titre, le FSD veille à la déclinaison et à la mise en oeuvre des dispositions relatives à la protection du potentiel scientifique et technique (PPST) qui s'inscrivent dans le cadre de procédures réglementaires nationales. Son action vise ainsi à protéger les laboratoires contre les atteintes à leurs intérêts économiques et contre les risques de détournement de travaux de recherche à des fins de prolifération ou de terrorisme.

Le FSD, en outre, participe à la protection du patrimoine informationnel de l'université en étroite liaison avec le RSSI. Il est en charge du déploiement des plans nationaux de défense et de protection, en particulier le plan VIGIPIRATE. A cet égard, il identifie et évalue les risques et propose des parades et s'assure de leur mise en oeuvre effective.

III.1.7 Le correspondant SSI

Chaque responsable de structure (directeur d'unité, de composante d'enseignement, de laboratoire, de pôle, direction ou service, ...) est responsable de la sécurité au sein même de sa structure, et doit par conséquent respecter les exigences SSI de l'université de Bordeaux. À ce titre il doit désigner un correspondant SSI pour sa structure. Ce dernier sera le correspondant direct du RSSI, dans le cadre des actions et projets menés conjointement.

Les activités possibles du correspondant SSI pourront être, selon le contexte :

- Piloter des analyses de risques de son entité
- Mettre en oeuvre des mesures de sécurité
- Diffuser en interne des bonnes pratiques
- Participer à la sensibilisation de la SSI auprès des usagers du SI

- Participer aux comités de sécurité organisés par le RSSI
- Participer à la déclinaison des exigences de sécurité sur son entité en coordination avec le RSSI
- Assurer le maintien en conditions de sécurité du SI de son entité : conception, déploiement, supervision, administration et exploitation du SI
- Participer aux traitements des incidents en coordination avec le RSSI et la DSI

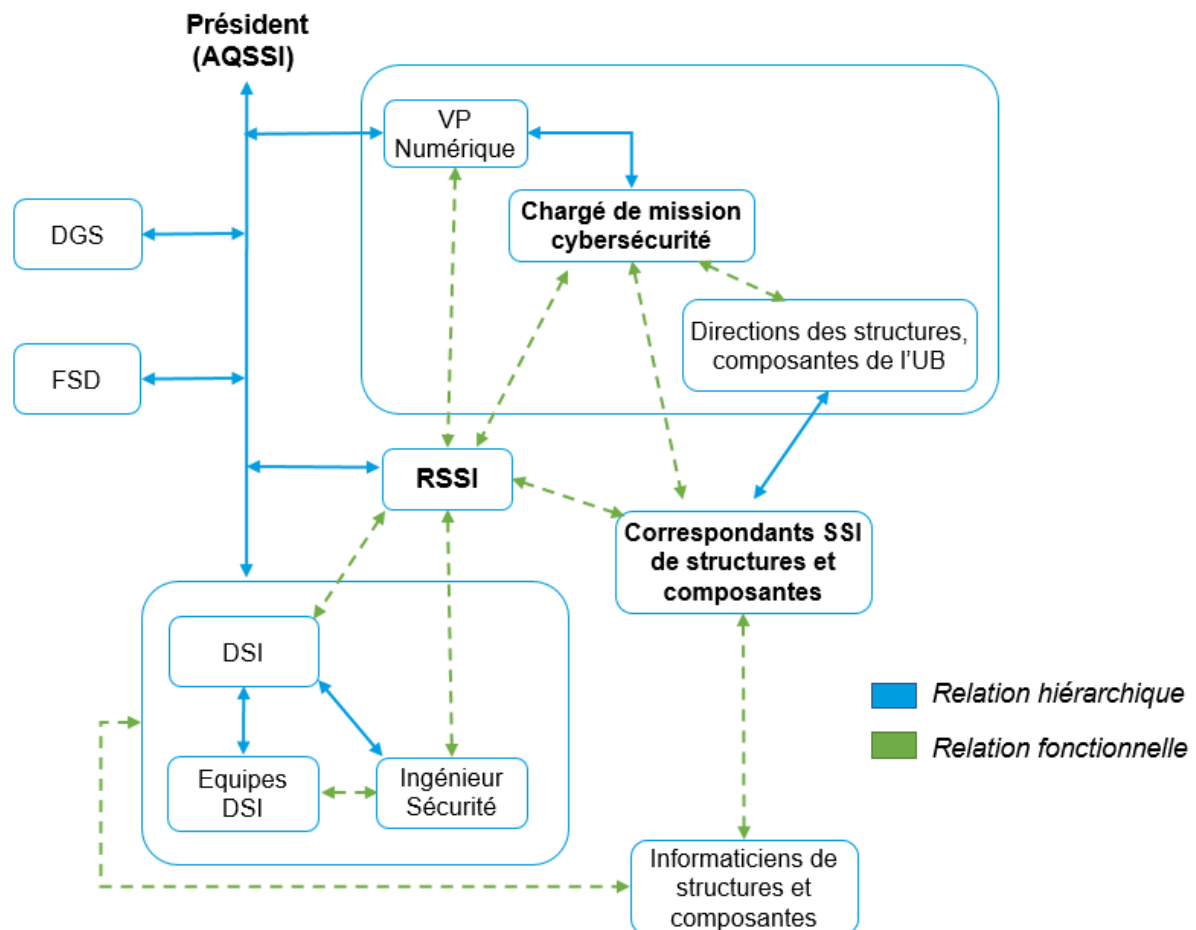


Figure 1 Organisation de la Sécurité des Systèmes d'Information

III.2 Instances de gouvernance de la sécurité

III.2.1 Le Comité stratégique de la sécurité des SI

Le comité stratégique, instance annuelle, composé des membres du Comité de Direction, du VP Numérique, du chargé de mission sécurité, de la DSI, du fonctionnaire de sécurité défense (FSD), du RSSI et du DPO, permet de partager et valider :

- La stratégie de la sécurité des systèmes d'information
- Une vision prospective sur l'évolution des risques cyber
- La feuille de route et les objectifs
- Le plan de traitement des risques

- Les moyens et ressources nécessaires à mettre en œuvre
- Les budgets nécessaires
- Les évolutions de la PGSSI

Ce comité est dirigé par le Président de l'université de Bordeaux, qui s'appuie sur le RSSI pour le pilotage du comité et son animation.

III.2.2 Le Comité de pilotage de la sécurité des SI

Le Comité de pilotage est une instance mensuelle permettant le pilotage et le suivi de la mise en œuvre des actions et des projets de SSI :

- Pilotage de la feuille de route SSI
- Suivi des projets et actions en cours
- Identification des évolutions nécessaires
- Suivi des indicateurs de pilotage

Le comité de pilotage est dirigé par le RSSI en coordination avec les Responsables de Direction en charge de la SSI (FSD, DPO, DSI, Chargé de mission SSI, VP Numérique...).

III.2.3 Le Comité de suivi de la sécurité des SI

Le comité de suivi est une instance bimensuelle sur demande du RSSI, permettant de suivre l'avancement des activités opérationnelles de sécurisation sur l'ensemble du système d'information :

- Suivi des actions de sécurisation
- Analyse des évènements et incidents de sécurité
- Amélioration des processus qualité

Le comité de pilotage est dirigé par le RSSI en coordination avec les correspondants SSI concernés, et les équipes de la DSI.

IV. Principes de mise en œuvre

Les principes de mise en œuvre s'articulent autour d'un pilotage et d'une démarche d'intégration de la sécurité du système d'information à tous les niveaux et d'une chaîne de responsabilité. Ils sont basés sur les activités suivantes :

- Engager les responsabilités, au travers de la gouvernance et du pilotage de la sécurité, de chaque structure et tiers utilisateurs du SI
- Identifier les risques et définir les mesures prioritaires
- Implémenter les mesures prioritaires
- Piloter la mise en œuvre et contrôler périodiquement le niveau d'application des mesures
- Identifier et mettre en œuvre des actions en fonction des écarts.

IV.1 Garantir la sécurité des SI

Chaque Responsable de structure (directeur de composante ou de service) et chaque partenaire de l'Université est **responsable de la sécurité de son entité**, et doit pouvoir présenter des garanties en la matière. Il doit assurer un niveau de sécurité et de résilience adapté aux activités qu'il porte, et suffisant pour ne pas compromettre les moyens et services numériques proposés par l'université de Bordeaux. Par conséquent, il est garant de la bonne gestion et maîtrise des actifs du SI (PC, équipements industriels, objets connectés, ...) auxquels son entité accède. Il répond de la présence légitime ou illégitime d'équipements non référencés et introduits sur le SI dans son périmètre d'activité, par un personnel de son entité ou par un tiers.

À cette fin, au regard des enjeux de SSI, en fonction des missions, des projets et attentes de chaque responsable d'entité, un ensemble d'exigences minimales à respecter, sera défini afin d'établir une zone de confiance favorisant la confidentialité, l'intégrité et la disponibilité de l'information.

Les réseaux de l'Université sont interconnectés avec le réseau national RENATER et au-delà à des réseaux internationaux (exemple le réseau GEANT).

La vigilance de l'université de Bordeaux contribue ainsi à la sécurité de la recherche nationale et internationale. Pour assurer la sécurité des SI, RENATER et l'Université déploient des outils d'analyse et de détection des menaces et attaques.

En cas de besoin, l'Université peut bloquer les communications sur le réseau, généralement en lien avec les administrateurs des équipements concernés. En cas d'urgence cela peut se faire sans délai.

IV.2 Identifier les risques et définir les mesures prioritaires

Les mesures de sécurité, quel qu'en soit le périmètre, doivent être définies au regard des risques spécifiques de SSI en lien avec la démarche globale du management des risques traités au sein même de l'université de Bordeaux.

Les risques majeurs doivent être identifiés et réévalués périodiquement en fonction de l'état du SI, de ses vulnérabilités, de l'évolution générale des menaces, et des impacts que la réalisation de ces menaces pourrait provoquer sur les actifs critiques. Pour ces raisons, les biens critiques doivent être identifiés et classifiés. La classification est appréciée selon les quatre critères de sécurité (disponibilité, intégrité, confidentialité, et traçabilité).

Le RSSI met en place une méthodologie d'évaluation et de traitement des risques, applicable à l'ensemble des systèmes d'information, et en coordination avec la direction pédagogique, les laboratoires, la DSI et la Présidence de l'université de Bordeaux. Cette dernière s'appuiera sur les évaluations et résultats d'analyses pour piloter le management des risques dans sa globalité (indicateurs de pilotage).

Le RSSI coordonne de manière régulière avec les correspondants SSI, les différentes analyses de risques à mener selon le périmètre du SI identifié (plate-forme, portail web, équipements des laboratoires, etc.) et nécessaires au regard de sa sensibilité, de ses évolutions, des nouveaux usages, et des contraintes réglementaires.

A l'issue de chaque évaluation, un plan de traitement est formalisé pour réduire les risques identifiés à un niveau acceptable.

En complément, des tests d'intrusions pourraient être réalisés périodiquement ou à chaque évolution majeure, afin de vérifier à minima la robustesse des systèmes d'information.

Les résultats des tests alimenteront les tableaux de bords, notamment la cartographie des risques.

IV.3 Intégrer la sécurité dans les projets

La sécurité des SI doit être prise en compte dans toutes les phases des projets informatiques, et sur l'ensemble du cycle de vie de ces derniers (MOA/MOE), dès la phase d'opportunité d'un projet.

Tout projet devra prendre en compte le principe de « security by design » stipulant que la SSI est prise en compte dès la phase de conception, et que cette dernière garantira la robustesse et le bon niveau de protection des composants (matériel, logiciel, données).

Cette exigence devra s'intégrer dans la démarche méthodologique des parties prenantes, afin de garantir le bon niveau de protection, de la phase de conception jusqu'à la mise en production.

La sécurisation sera atteinte par la mise en œuvre de mesures proportionnées et adaptées visant à assurer le niveau de sécurité requis en terme de :

- **Confidentialité** : capacité à protéger les informations de toute diffusion et divulgation à des personnes, des entités ou des processus non autorisés.
- **Intégrité** : capacité à préserver les informations de toute altération, destruction ou modification non autorisée.

- **Disponibilité** : capacité à maintenir l'accessibilité aux informations et aux applications dans des conditions d'horaire et de délai attendues.
- **Traçabilité** : capacité à enregistrer et à conserver des logs systèmes et les traitements des informations selon la réglementation et les politiques de sécurité.

Dans le cadre d'un recours à un fournisseur ou un prestataire, les exigences de sécurité pourront être complétées par un Plan d'Assurance Sécurité (PAS). Ce document indiquera les engagements et les mesures de sécurité du fournisseur en matière de protection et de sécurité du système d'information concerné.

IV.4 Gérer les incidents SSI

L'objectif est de définir une organisation cohérente, coordonnée et efficace de gestion des incidents liés à la sécurité de l'information, incluant :

- La communication des événements et des failles liées à la sécurité
- Des enregistrements des événements et traces liés aux incidents
- Une capitalisation par des actions correctives et préventives

En relation directe avec les correspondants SSI de chaque entité, le RSSI avec la DSI, reçoit et analyse les remontées d'alertes, et appuie le cas échéant, les correspondants SSI dans la qualification des incidents. Le traitement des incidents sera porté soit par la DSI et ses équipes soit par les informaticiens des partenaires, en coordination avec le RSSI. Cette centralisation permettra d'améliorer la réactivité nécessaire en cas d'attaque informatique.

En cas **d'incident majeur ou de situation de crise**, impactant fortement les activités de l'université de Bordeaux, **une cellule de crise sera activée**, impliquant l'ensemble des acteurs permettant de remédier à la situation, et de gérer la crise. Cette cellule pourra en coordination avec le RSSI, s'appuyer sur les services de l'État et les partenaires concernés.

IV.5 Contrôler et assurer la conformité

L'université de Bordeaux souhaite s'inscrire dans une démarche de conformité et de respect du cadre réglementaire. A ce titre, et au regard des exigences de conformité, l'université de Bordeaux s'appuie sur la politique de sécurité de l'État, la PSSI-E, et celle de son ministère de tutelle, la PSSI-M.

IV.5.1 Cadre réglementaire et conformité

Le Référentiel Général de Sécurité (RGS v2.0)

En tant qu'Autorité Administrative comme tout établissement public, l'université de Bordeaux est tenue de respecter le Référentiel Général de Sécurité établi par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), officialisé par le décret n° 2010-112 du 2 février 2010.

À ce titre, l'université de Bordeaux doit mener à bien les homologations nécessaires, afin d'attester formellement auprès des utilisateurs de son système d'information que celui-ci est sécurisé conformément aux objectifs de sécurité fixés.

La Loi de Programmation Militaire

Compte-tenu des enjeux en matière de protection de l'information, l'université de Bordeaux est tenue de prendre en compte les exigences et contraintes relatives à la sécurité des systèmes d'information des opérateurs d'importance vitale, ces derniers pouvant être partenaires dans des projets de recherche notamment.

À ce titre, elle doit sécuriser ses Systèmes d'Information, afin d'attester que ceux-ci sont protégés conformément aux objectifs de sécurité fixés entre les parties. Elle doit également désigner un officier de sécurité à qui incombe l'organisation, la gestion et le contrôle interne de la protection des informations et supports classifiés et de l'application de la réglementation.

Protection des données à caractère personnel (RGPD)

Pour l'ensemble de ses activités, l'université de Bordeaux participe à la mise en œuvre de traitements de données à caractère personnel. À ce titre, l'université de Bordeaux doit s'assurer que ces traitements sont réalisés conformément aux exigences de la Loi Informatique et Libertés (loi 78/17), ainsi qu'au règlement EU 2016/679 dont la date d'applicabilité est définie au 25 mai 2018.

Réglementation Hébergement des données de santé (HDS)

L'université de Bordeaux héberge son système d'information et les plates-formes le cas échéant des structures et autres entités. Au regard de la typologie des données, et dans le cadre des activités de recherche, l'obligation d'être certifiés HDS par un organisme accrédité peut s'avérer nécessaire, et l'université de Bordeaux pourra s'inscrire dans cette démarche ou s'appuyer sur un hébergeur certifié.

IV.5.2 Audits internes

Afin de satisfaire au cadre réglementaire, et de vérifier l'application correcte des principes et règles de sécurité émanant de la PGSSI et de tout document relatif à la déclinaison de cette dernière, au travers de directives et actions de sécurité à mener au sein des entités, des contrôles pourront être menés sous la responsabilité du RSSI. Ces contrôles auront pour but notamment d'apporter une meilleure cohérence, et d'évaluer le niveau de maturité sur l'ensemble des entités, afin d'améliorer la résilience de l'université de Bordeaux, de ses partenaires et de tous bénéficiaires du système d'information et services associés.

En complément des contrôles ponctuels évoqués, des audits relatifs au cadre réglementaire, de conformité ou audits internes à l'appréciation du RSSI et en coordination avec l'équipe du contrôle d'audit interne, seront programmés sur l'année, pour analyser et évaluer la pertinence des mesures, l'efficacité des organisations et moyens mis en œuvre. Ces différents audits pourront être aussi menés par des prestataires référents en la matière selon la nécessité, pour appuyer les activités d'audit.

Tout partenaire ou tiers pourra être audité à la demande du RSSI, pour s'assurer du respect des politiques de sécurité des SI et vérifier la bonne application des mesures et les moyens déployés, au regard des enjeux de sécurité, et des niveaux de risques évalués périodiquement.

Concernant la qualification et le référencement des prestataires, fournisseurs, éditeurs et partenaires technologiques externes, ces derniers devront pouvoir apporter des garanties, et démontrer leur capacité à répondre aux exigences de sécurité, exprimées dans l'annexe de sécurité des appels d'offres et marchés de l'Université, précisant notamment, l'acceptation de chacun à pouvoir être audité et contrôlé pendant toute la durée de la relation contractuelle.

Par conséquent, des audits seront réalisés par le RSSI pour vérifier l'application des exigences de sécurité de l'université de Bordeaux, et la pertinence des moyens déployés.

IV.5.3 Réévaluer la PGSSI

La politique devra faire l'objet d'une revue périodique visant à valider son champ d'application ainsi que l'ensemble des principes énoncés et essentiels au regard des enjeux de sécurité des SI. Cette réévaluation devra avoir lieu une fois tous les 2 ans, voire dans un délai plus court si elle est motivée et justifiée par une évolution du contexte et de l'environnement de l'université de Bordeaux. Elle sera portée par le RSSI.

La révision de la PGSSI, imposera de réévaluer les impacts sur le corpus documentaire, et notamment la pertinence des politiques thématiques suivantes :

- Politique de mot de passe
- Politique de chiffrement
- Politique de traitement des vulnérabilités
- Politique de gestion des actifs
- etc

En savoir +

www.u-bordeaux.fr



@ univbordeaux



univbordeaux



universitedebordeaux



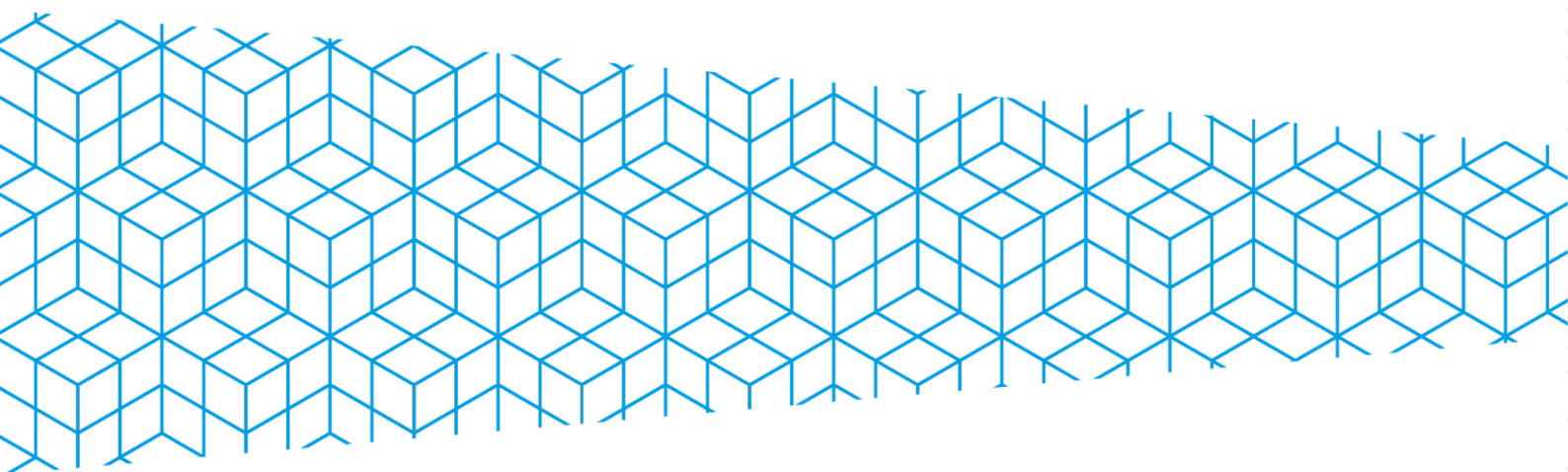
universite-de-bordeaux

université
de **BORDEAUX**

Charte informatique

Version : 1.0

Date de publication : 30/05/2023



Version	Auteurs	Commentaires	Date de publication
V1	Soben CHHEM (RSSI) Jean-Marc COUVEIGNES (Chargé de mission sécurité) Contributions : Karim BELEBAS (VP Numérique) Frédéric POMIES (Directeur des Systèmes d'Information) Xavier DAVERAT (DPO) Direction des affaires juridiques	Version initiale du document	30/05/203

Vu l'avis du comité social d'administration du 12/05/2023

Vu la délibération du conseil d'administration du 23/05/2023

Table des matières

Définitions.....	3
Table des matières	3
Définitions	5
I. Préambule	7
II. Champ d'application et sanctions	8
III. Opposabilité, entrée en vigueur	8
IV. Conditions d'utilisation	9
IV.1 Utilisation professionnelle / privée.....	9
IV.2 Gestion des absences et continuité de service	9
IV.3 Journalisation et contrôles.....	9
IV.4 Interdictions.....	10
V. Principes de sécurité	11
V.1 Autorisation d'accès.....	11
V.2 Accès à distance	11
V.3 Gestion des identifiants et des mots de passe	11
V.4 Sécurité du système d'information.....	12
V.5 Utilisation des supports amovibles	13
V.6 Accès à l'Internet	14
V.7 Utilisation de services « Cloud »	15
V.8 Publication sur le site internet de l'Université.....	15
V.9 Devoirs de signalement et d'information	15
V.10 Dysfonctionnement, maintenance	16
VI. Protection des données.....	16
VI.1 Informations et données professionnelles	16
VI.2 Données confidentielles et sensibles.....	16
VI.3 Zones à régime restrictif « ZRR »	17
VI.4 Données à caractère personnel	17
VII. Communication numérique.....	18
VII.1 Messagerie électronique	18
VII.2 Adresse électronique	18
VII.3 Contenu des messages.....	18
VII.4 Emission et réception des messages	19

VII.5	Stockage et archivage des messages	19
VII.6	Sécurité de la messagerie	19
VIII.	Protection des mineurs	20
IX.	Propriété intellectuelle	20
	Quelques textes de référence applicables	21

Définitions

Dans cette Charte, on entend par :

Administrateur : Tout agent ou sous-traitant ayant pour mission d'assurer l'administration d'un ou plusieurs systèmes informatiques.

CSN (Centre de Support Numérique) : Le centre de support numérique est le point d'entrée pour les demandes d'assistance et alertes émises par les utilisateurs. Il distribue les sollicitations aux équipes compétentes.

CSSI (Correspondant pour la sécurité des systèmes d'information) : Le CSSI est l'interlocuteur privilégié du RSSI pour sa structure. Il relaie les messages d'information et de sensibilisation. Il accompagne les personnels de sa structure pour les aspects SSI de leurs métiers.

Donnée à caractère personnel : Toute information relative à une personne physique susceptible d'identifier celle-ci directement ou indirectement.

Equipement nomade : Tout support informatique mobile, et notamment : ordinateur portable, tablette tactile, téléphone portable, smartphone (téléphone multifonctions), clé USB, CD ROM, disque dur externe, etc.

RSSI (Responsable de la sécurité des systèmes d'information) : Le RSSI formalise la politique de sécurité des systèmes d'information. Il organise et coordonne sa mise en œuvre.

Service numérique : Ensemble cohérent de **ressources** humaines, matérielles et logicielles mobilisées et orchestrées en vue de permettre à l'utilisateur de réaliser une ou plusieurs tâches professionnelles informatisées. Exemples :

- La fourniture d'équipements informatiques et téléphoniques
- La connectivité au réseau Wi-Fi ou filaire
- La mise à disposition d'applications informatiques prêtes à l'usage
- Le développement d'applications informatiques
- Etc.

Structure : La structure d'un utilisateur est la composante d'enseignement, l'unité de recherche, la direction, le pôle, le service administratif ou toute entité dont relève son activité.

Système d'information (SI) : Ensemble des services numériques mis en œuvre et des données associées, notamment et non exclusivement les matériels, logiciels, applications, bases de données, services, réseaux, objets nomades.

Université : L'Université de Bordeaux.

Utilisateur : Toute personne accédant au système d'information de l'Université, notamment et non exclusivement les personnels titulaires ou contractuels de l'Université, les étudiants, les personnels

des partenaires, clients ou prestataires de l'Université, les visiteurs, les invités, les intervenants extérieurs, etc.

ZRR (Zones à régime restrictif) : Zones protégées afin d'empêcher que des éléments essentiels du potentiel scientifique ou technique de la nation :

- fassent l'objet d'une captation de nature à affaiblir ses moyens de défense, à compromettre sa sécurité ou à porter préjudice à ses autres intérêts fondamentaux;
- ou soient détournés à des fins de terrorisme, de prolifération d'armes de destruction massive et de leurs vecteurs ou de contribution à l'accroissement d'arsenaux militaires.

Ces zones sont précisément délimitées et explicitement signalées.

I. Préambule

L'Université de Bordeaux met en œuvre un système d'information et de communication nécessaire à la réalisation de ses missions. Ce système est un outil de partage de connaissances, un facteur d'excellence de l'enseignement et de la recherche et un instrument majeur des transitions environnementales et sociétales.

Ce système d'information, composé de nombreux logiciels et appuyé sur des réseaux interconnectés à l'échelle mondiale, constitue une cible de choix pour les cyberattaques.

L'Université met en œuvre les moyens humains et matériels propres à assurer la sécurité de son système d'information et à son amélioration. Elle est responsable du contrôle du bon fonctionnement dudit système et veille à l'application des dispositions de la présente charte.

L'utilisateur est responsable de l'usage qu'il fait du système d'information et notamment des services numériques mis à sa disposition. Il concourt à la sécurité par l'application des règles édictées par la présente Charte, par sa vigilance et sa prudence.

L'utilisation des services numériques soulève la double contrainte de la protection de l'information traitée par les utilisateurs et des ressources qui composent le système d'information de l'Université.

Les mesures mises en œuvre pour répondre à cette double nécessité doivent permettre à l'Université de remplir ses missions et de satisfaire en même temps aux exigences imposées :

- Par ses engagements vis-à-vis de ses partenaires
- Par le respect de la réglementation sur la protection des données sensibles et la protection du patrimoine scientifique
- Par le respect des dispositions légales en matières civile et pénale
- Par le respect de la loi sur la protection des données personnelles
- Par la nécessité de maîtriser le coût et l'impact environnemental des services numériques.

L'élaboration des règles d'utilisation et la mise en œuvre des contrôles associés, l'information et la sensibilisation des personnels et étudiants sont donc indispensables.

Cette charte vise à informer les utilisateurs de leurs droits et de leurs devoirs. Il est entendu que l'application de la présente charte se fait dans le respect du décret n°82-447 du 28 mai 1982 relatif à l'exercice du droit syndical dans la fonction publique et de la charte de l' élu en vigueur au sein de l'établissement et de tout document qui viendrait à s'y substituer.

II. Champ d'application et sanctions

La présente charte s'applique à tous les utilisateurs du système d'information de l'Université.

Elle concerne l'ensemble des équipements et logiciels informatiques et audiovisuels et notamment :

- Ordinateurs fixes et mobiles
- Téléphones fixes, mobiles, smartphones, tablettes
- Copieurs, imprimantes, scanners
- Terminaux de visioconférence, zoomrooms, vidéoprojecteurs, écrans, solutions de captation assistées et autonomes
- Logiciels, applications en ligne, sites web, plateformes numériques internes et externes
- Interfaces programmatiques (API), flux de données

La liste n'est pas exhaustive et se limite à illustrer le périmètre global.

Certains services numériques (la téléphonie mobile professionnelle, UBCloud, ...) sont encadrés par des règles ou des conditions générales d'utilisation (CGU) spécifiques. Certaines activités requièrent un usage spécifique du numérique (le télétravail, les élections par voie électronique, la communication des organisations syndicales, ...). En conséquence, la présente charte s'applique sans préjudice de ces autres cadres, elle vise à les compléter. Les politiques et directives de sécurité sont consultables sur l'intranet et sur le site institutionnel de l'Université.

Chaque utilisateur applique les prescriptions de cette charte et se conforme aux recommandations et aux directives des administrateurs des systèmes d'information et du RSSI.

Il est tenu au respect des lois, des règlements et des obligations statutaires, déontologiques, éthiques et contractuelles le concernant.

L'Université ne pourra être tenue pour responsable des détériorations ou des manquements commis par un utilisateur qui ne se sera pas conformé à ces règles. Tout manquement à ces stipulations engage la responsabilité personnelle de l'utilisateur.

Tout manquement peut donner lieu à :

- **Une limitation ou une interdiction d'accès à ses ressources numériques**
- **La suppression d'une donnée en contradiction avec la charte ou préjudiciable au bon fonctionnement des systèmes d'information**
- **Des sanctions disciplinaires et des poursuites pénales.**

III. Opposabilité, entrée en vigueur

La présente charte sera intégrée au règlement intérieur de l'Université de Bordeaux dont elle sera une annexe. Elle est applicable à compter de son approbation par les instances de l'Université (le comité social d'administration et le conseil d'administration).

IV. Conditions d'utilisation

IV.1 Utilisation professionnelle / privée

La présente Charte qualifie de professionnelle l'utilisation des services numériques :

- dans le cadre des missions confiées à l'utilisateur par l'Université ou par son employeur ;
- dans le cadre des activités pédagogiques pour les utilisateurs étudiants.

Toute autre utilisation est qualifiée de privée.

L'utilisateur utilise les services numériques que l'Université met à sa disposition à seules fins professionnelles. Il fait un usage raisonnable de ces services notamment en termes de puissance de calcul, espace mémoire, bande passante et toute ressource partagée ou limitée. Il s'abstient de perturber le bon fonctionnement du système d'information.

Toutefois, une utilisation privée est autorisée dans les cas d'urgence et de nécessité. En outre, elle est tolérée sous réserve qu'elle soit conforme aux dispositions de cette charte et en particulier aux principes de sécurité. Elle doit être limitée en fréquence comme en durée et non lucrative. Elle ne doit pas mobiliser une part excessive des moyens numériques. Son coût pour l'Université doit être négligeable. Elle ne doit pas nuire au bon fonctionnement de l'Université. Elle ne peut engager la responsabilité de l'Université. Elle ne doit pas porter atteinte à son image ou à sa réputation. Elle ne doit pas affecter la qualité du travail de l'utilisateur ni le temps qu'il y consacre. Elle doit être conforme aux lois, règlements et dispositions internes.

IV.2 Gestion des absences et continuité de service

L'utilisateur est responsable de son espace de données à caractère privé. Lors de son départ définitif de l'établissement, il lui appartient de veiller à la mise à disposition de ses données professionnelles utiles à la continuité de service, de récupérer et supprimer ses données privées, la responsabilité de l'Université ne pouvant être engagée quant à la conservation de cet espace.

Chaque équipe doit prendre toutes les dispositions de transmission de données nécessaires à la continuité de service, dans le respect de la sécurité et de la confidentialité.

Cela vaut notamment pour les accès institutionnels à des réseaux sociaux, et à des plateformes externes gérant leurs propres accès.

En cas de nécessité, et notamment en cas de départ ou d'absence de l'utilisateur, l'Université se réserve le droit d'accéder directement à ses données professionnelles, si nécessaire avec le concours de l'administrateur du système d'information.

IV.3 Journalisation et contrôles

Aucune cyber surveillance généralisée n'est mise en place à l'Université.

Certaines zones des campus sont équipées de dispositifs de vidéo protection. Ces dispositifs, placés sous la responsabilité stricte de la direction en charge de la sûreté, entrent dans le cadre réglementaire prévu. Aucune exploitation des données ne peut être faite en dehors de ce cadre.

L'utilisateur des services numériques est informé que l'ensemble des opérations (accès, usages) informatiques et électroniques laisse des traces exploitables en temps réel ou différé. L'Université se réserve le droit de mettre en place, sur tous les services numériques qu'elle met à sa disposition, des dispositifs de collecte des traces aux fins de supervision du bon fonctionnement, de contrôle, de sauvegarde et de journalisation à des fins statistiques, de traçabilité réglementaire ou fonctionnelle, de recherche de panne, d'optimisation, d'audit, de sécurité ou de détection des abus.

Les traces enregistrées alimentent les fichiers de journalisation qui comportent au minimum la date, l'identifiant et le type d'événement. Ils fonctionnent sur le principe de l'ajout exclusif, c'est-à-dire que chaque action de l'utilisateur ajoute une trace supplémentaire, aucune action de l'utilisateur ne conduit à supprimer une trace. Les fichiers de journalisation sont conservés au maximum douze mois sauf contraintes réglementaires. Ils sont exclusivement destinés à l'Université et aux autorités habilitées. Les personnels qui les utilisent sont soumis à une obligation de confidentialité.

Les dispositifs qui opèrent des restrictions d'accès enregistrent les traces des tentatives non autorisées. Il s'agit notamment du système de contrôle d'accès des campus et de bâtiments, des systèmes d'authentification et des pare-feu. Les tentatives non autorisées sont susceptibles de déclencher des comportements préventifs automatisés qui peuvent aller jusqu'à isoler les postes de travail, smartphones, tablettes concernés.

Conformément au Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD) et à la loi numéro 78-17 du 6 janvier 1978 dite *Informatique et Libertés* modifiée, ce traitement de données sera inscrit au registre des traitements de l'Université. L'utilisateur peut obtenir des précisions concernant ce registre auprès du délégué à la protection des données (voir la section VI.4).

IV.4 Interdictions

L'utilisateur s'interdit expressément d'utiliser quelque élément que ce soit du système d'information de l'Université aux fins de consulter, échanger, charger, stocker, diffuser ou faire suivre des fichiers, images, informations ou communications de toute nature :

- contraire à la législation en vigueur en France ou à l'ordre public, et notamment contenant des éléments à caractère violent, pornographique ou pédophile;
- à caractère discriminatoire, raciste, sexiste, révisionniste ou incitant à la haine;
- portant atteinte aux droits de la personnalité, qu'il s'agisse de la vie privée ou du droit à l'image des personnes physiques, sauf à avoir obtenu l'autorisation expresse des intéressés, laquelle doit comporter le cadre et les limites précises de ladite autorisation;
- portant atteinte au secret des correspondances;
- portant atteinte à la dignité des personnes;
- portant atteinte à la protection des mineurs;
- à caractère diffamatoire;
- portant atteinte à un droit de propriété intellectuelle tel que visé en section IX ci-après;

- en violation des dispositions relatives aux données à caractère personnel;
- en violation du secret attaché à certaines informations (secret professionnel, secret médical, etc.);
- contraire à des règles de déontologie ou des principes éthiques.

L'utilisateur procède à la suppression immédiate de tout élément qu'il a reçu et qui lui apparaît comme portant atteinte à un des droits ou intérêts visés ci-dessus.

V. Principes de sécurité

Les règles de sécurité visent à garantir le bon fonctionnement du système d'information et à protéger la confidentialité, l'intégrité et la disponibilité des informations. Tout manquement à ces règles peut avoir des conséquences graves (humaines, scientifiques, juridiques, financières, environnementale).

V.1 Autorisation d'accès

Toute mise en interaction de systèmes informatiques (équipements, accès aux réseaux, recueils de logs, supports amovibles ...), doit se faire dans le strict respect de l'ensemble des dispositions de la présente charte, notamment des principes de sécurité et des obligations de confidentialité. Elle ne doit pas perturber le fonctionnement du système d'information de l'Université ni affaiblir sa sécurité.

L'accès et l'utilisation des services numériques de l'Université, notamment l'octroi d'une identité numérique de l'Université « IDNUM » et l'accès au SI de l'Université, sont soumis à autorisation ou aux accords contractuels.

Toute autorisation prend fin lors de la cessation de l'activité professionnelle ou du contrat qui l'a justifiée, sauf cas particulier, ainsi qu'en cas de manquement grave ou répété à la présente charte.

L'interconnexion au SI de l'Université doit faire l'objet d'une validation préalable par la DSI ou par un tiers avec sa délégation, qui vérifie la conformité. Il est de la responsabilité de l'utilisateur ou de l'établissement employeur de s'en assurer.

V.2 Accès à distance

Le principe général est que l'accès au système d'information, hors du réseau informatique local – hors des locaux de l'université, doit se faire avec le VPN (réseau privé virtuel).

Par exception, pour des raisons de productivité professionnelle dans un contexte de nomadisme croissant, certains composants du système d'information sont directement accessibles depuis l'Internet (messagerie électronique, gestion des commandes, etc.).

En fonction de l'évolution des menaces cyber, le périmètre des traitements d'exception peut faire l'objet d'adaptations rapides.

V.3 Gestion des identifiants et des mots de passe

Lorsque l'accès à un système se fait avec un mot de passe initial celui-ci doit être changé à la première utilisation par son utilisateur, dans le respect des prescriptions ci-dessous. Le mot de passe déterminé par l'utilisateur ne doit pas être facilement déterminable, par déduction, et ne doit notamment pas être constitué des mêmes caractères que l'IDNUM, l'identité de l'utilisateur, un numéro de téléphone, un numéro d'immatriculation de véhicule, etc.

La complexité minimale des mots de passe est paramétrée par l'équipe DSI et les informaticiens de laboratoires et composantes dans les systèmes d'information respectivement sous leur gestion. Lorsque ce n'est pas le cas, le mot de passe doit comporter au minimum 8 caractères alphanumériques, des majuscules, minuscules et des caractères spéciaux.

Pour des raisons d'activités métiers, certains accès disposent d'un compte partagé (identifiant et mot de passe) dont la diffusion et la gestion est de la responsabilité du Responsable de service concerné. Ce dernier doit être en mesure de tracer l'affectation de ce compte partagé.

Les identifiants et mots de passe de chaque utilisateur (IDNUM, comptes applicatifs ...) sont strictement personnels et confidentiels. Les mots de passe ne doivent en aucun cas être dévoilés à quiconque, y compris au service informatique ou à tout organe de gouvernance de l'Université. L'utilisateur est seul et totalement responsable de l'utilisation et de la confidentialité du mot de passe.

Les mots de passe doivent être soit mémorisés par l'utilisateur, soit conservés dans un coffre-fort ou un coffre-fort électronique les conservant sous forme chiffrée (logiciel de gestion des mots de passe tel que Keeypass). Toute autre forme de stockage, informatique ou papier, est strictement interdite. La fonction de mémorisation du mot de passe, dans les navigateurs Web notamment, est à proscrire.

L'utilisateur saisit généralement son identifiant et mot de passe sur le service central d'authentification (**CAS** - <https://cas.u-bordeaux.fr>) de l'Université ou des applications web habituelles qui finissent par **u-bordeaux.fr**. Il vérifie préalablement l'adresse de ces sites dans la barre de navigation.

Il est strictement interdit de laisser les mots de passe par défaut dits « usine » sur tout type de ressources.

Les identifiants et mots de passes utilisés pour les activités professionnelles, ne doivent jamais être utilisés dans d'autres cadres notamment personnel (sites Internet, messagerie personnelle telle que Gmail, sites d'achat ...).

Toute action effectuée par l'utilisateur, à l'aide de son identifiant est imputable et engage sa responsabilité. L'utilisateur ne doit en aucun cas faire usage des moyens d'authentification ou des habilitations d'une tierce personne.

L'authentification par clé cryptographique (usage répandu chez les informaticiens) est assimilée à une authentification individuelle. L'usage et la conservation des clés cryptographiques doivent bénéficier du même soin que les identifiants et mots de passe.

V.4 Sécurité du système d'information

L'utilisateur respecte les dispositifs mis en place par l'Université pour protéger le système d'information. Il ne modifie pas la configuration de son poste de travail et ne doit jamais désactiver ou tenter de contourner les mécanismes de protection mis à sa disposition (antivirus, pare-feu, mise à jour de sécurité, etc.)

Il utilise les moyens matériels et logiciels disponibles pour protéger les équipements (câbles antivol, rangements fermés à clé, chiffrement des équipements mobiles, etc.)

Il s'interdit de télécharger, installer, utiliser des logiciels ou services dont les droits de licence n'ont pas été acquittés pour cet usage, ou qui ne proviendraient pas de sites de confiance.

Dans tous les cas il sollicite l'accord de sa structure ou de l'administrateur compétent avant d'installer un logiciel.

En cas d'absence, même brève, il verrouille ou ferme les sessions en cours sur son poste de travail et sur tout matériel contenant des données professionnelles.

Il applique les bonnes pratiques de sécurité issues de la politique de sécurité des systèmes d'information de l'Université.

V.5 Utilisation des équipements nomades

Les équipements nomades (tels que définis au début de ce document) sont particulièrement vulnérables du fait de leur mobilité. S'ils facilitent le transport de données, ils représentent une menace importante en cas de perte, de vol ou de connexion sur les SI de l'Université. Ils augmentent le risque de vol d'identifiants et d'usurpation d'identité, et sont plus exposés à l'introduction de virus ou logiciels malveillants.

a) Usage des équipements nomades :

Le matériel nomade confié à l'utilisateur par la DSI bénéficie de protections spécifiques. Ne disposant pas des droits d'administrateur, l'utilisateur ne peut modifier la configuration effectuée par la DSI. Il s'interdit de modifier les paramètres du matériel et s'engage à répondre aux sollicitations de la DSI aux fins de mise à jour (applications, antivirus, etc.)

Les supports de stockage et outils de transfert de fichiers mis à disposition par l'Université doivent être privilégiés à tout autre.

L'utilisation des équipements nomades mis à disposition par l'Université respecte les dispositions de la section IV.1.

En cas d'usage de matériel nomade dans le cadre du télétravail, l'utilisateur se soumettra sans restriction aux dispositions de la *Charte du télétravail* de l'Université de Bordeaux.

b) Responsabilité de l'utilisateur :

L'utilisateur a la garde et la responsabilité du matériel nomade qui lui a été confié. Il s'oblige à fournir un niveau de surveillance renforcé. Il est responsable des données qui sont stockées sur ces équipements. Les informations confidentielles contenues sur ces équipements doivent être chiffrées selon les moyens mis à disposition par l'Université. L'utilisateur veille à ce que des tiers non autorisés ne puissent utiliser les équipements nomades qui lui sont confiés.

L'utilisateur est tenu de ne pas laisser les équipements sans surveillance dans des lieux dont l'accès n'est pas contrôlé, et de faire preuve d'une vigilance particulière dans les lieux publics et les transports en commun. Il active les écrans de veille et fixe un délai de verrouillage automatique des ordinateurs portables, tablettes tactiles, téléphones et smartphones.

L'utilisateur s'assure que les données à caractère professionnel sont sauvegardées sur le système d'information de l'Université. Il efface les données présentes sur les équipements nomades dès lors qu'elles ne sont pas immédiatement utiles. Il est invité à utiliser le service Cloud offert par l'Université.

V.6 Accès à l'Internet

Le réseau informatique de l'université de Bordeaux est relié par l'intermédiaire du Réseau RENATER (Réseau National de télécommunications pour la Technologie, l'Enseignement et la Recherche) à une communauté d'utilisateurs travaillant dans le domaine de l'éducation, de la recherche et de la technologie.

L'utilisateur s'engage à prendre connaissance et à respecter la charte « Charte de bon usage de l'informatique et du réseau RENATER », annexée à la présente charte, ou à tout document qui viendrait s'y substituer.

L'Université met à la disposition des utilisateurs un accès internet destiné à un usage professionnel. Une utilisation privée résiduelle est possible dans les limites énoncées à la section IV et sous réserve que le contenu des sites visités soit conforme à la loi et ne compromette pas la réputation de l'Université

L'Internet est soumis à l'ensemble des règles de droit en vigueur.

L'Université se réserve le droit de limiter ou d'interdire l'accès à certains sites et de procéder au contrôle a priori ou a posteriori des sites visités. Les utilisateurs ne peuvent accéder à l'Internet qu'au travers des dispositifs de sécurité et de contrôle mis en place par l'Université. Ces dispositifs sont notamment constitués de technologies de filtrage des flux réseau (pare-feu) et de prévention d'intrusion (IPS) qui analysent « en temps réel » les flux réseau, autorisent certains flux, en bloquent d'autres et notifient des alertes en cas de flux anormaux.

Dans le cadre d'une utilisation professionnelle ou privée de l'Internet, l'utilisateur veille au respect des prescriptions de la section VI concernant la protection des données. Il applique les recommandations de la *Charte du bon usage du numérique pour améliorer la qualité de vie au travail de tous* et du *Guide des bonnes pratiques pour l'usage des outils numériques de l'Université*.

Il ne se connecte pas volontairement à des sites Internet malveillants.

Pour participer à un réseau social, créer un espace ou un site au titre de l'Université ou de sa structure, l'utilisateur doit obtenir l'autorisation préalable de son directeur de structure. Il doit ensuite se conformer aux instructions de ce dernier et à la politique de communication de l'Université. Il doit obligatoirement renvoyer aux Conditions générales d'utilisation, à la politique de confidentialité et aux mentions légales en vigueur à l'Université

V.7 Utilisation de services « Cloud »

Les services cloud, dont certains sont gratuits, permettant très facilement aux utilisateurs de créer des espaces permettant la production, le stockage et le partage de documents et données ne doivent pas être utilisés pour y enregistrer des données professionnelles en lien avec l'Université.

En application de la circulaire n° 6282-SG du 5 juillet 2021 relative à la doctrine d'utilisation de l'informatique en nuage par l'État, les services cloud utilisés à l'Université doivent être conforme à la qualification SecNumCloud, au RGPD et, le cas échéant, à la législation sur l'hébergement des données de santé.

V.8 Publication sur le site internet de l'Université

Les directeurs de publication des sites internet ou intranet de l'université et de ses composantes se réservent le droit de modifier ou de supprimer tout contenu non conforme à la législation en vigueur, aux valeurs de l'université de Bordeaux ainsi qu'à leur ligne éditoriale.

La publication d'informations ou de pages d'information privées sur les serveurs de l'Université n'est pas autorisée.

V.9 Devoirs de signalement et d'information

L'utilisateur est tenu de signaler au Centre de Support Numérique dans les plus brefs délais tout évènement ou comportement de sécurité inhabituel qu'il serait amené à observer tels que :

- Une tentative d'intrusion ou le constat d'une intrusion
- L'utilisation ou la tentative d'utilisation d'un poste de travail par un inconnu, la connexion d'un équipement informatique étranger par un inconnu sur les réseaux informatiques de l'Université.
- Tout logiciel, dispositif, comportement suspect et toute atteinte ou tentative d'atteinte aux moyens d'information (dégradation, vol de matériel ou de données, altération, intrusion physique ou logique, etc.)

Le Centre de Support Numérique peut être contacté à l'adresse csn@u-bordeaux.fr

En cas de perte ou de compromission de ses moyens d'authentification l'utilisateur les renouvelle dès que possible et prévient sans tarder le CSSI de sa structure et le RSSI.

Il informe également le CSSI de sa structure ou le RSSI en cas de perte ou de vol d'un équipement informatique qui lui a été confié.

Le RSSI peut être contacté à l'adresse rsi@u-bordeaux.fr

Il assiste l'Université dans les démarches consécutives à tout incident concernant un moyen informatique mis à sa disposition (témoignage ou dépôt de plainte en cas de vol par exemple). En cas de sinistre, incident majeur ou autre nécessité absolue, l'Université peut restreindre, suspendre ou supprimer certains services.

V.10 Dysfonctionnement, maintenance

Les services informatiques de l'Université opèrent, sans avertissement, les investigations et actions nécessaires à la résolution de dysfonctionnements des systèmes d'information. Ils s'appuient pour ce faire sur les fichiers de journalisation.

Toute information bloquante ou dangereuse (virus, logiciel malveillant, pourriel, etc.) est susceptible d'être supprimée immédiatement.

Dans le cadre des opérations de maintenance, l'Université intervient (éventuellement à distance) sur les ressources mises à la disposition des utilisateurs. L'utilisateur est informé préalablement à toute opération de maintenance à distance.

Préalablement à son départ définitif l'utilisateur doit restituer l'ensemble des matériels et informations mis à sa disposition par l'Université et s'engage à ne pas conserver de copie.

VI. Protection des données

VI.1 Informations et données professionnelles

Toute information, tout fichier, répertoire ou dossier, ainsi que tout message est considéré comme professionnel sauf mention explicite de son caractère privé. Par exemple le champ *Objet* d'un message électronique privé doit commencer par le mot *privé*. Les données à caractère privé doivent être stockées dans un espace explicitement désigné comme privé. Cet espace ne doit pas contenir de données professionnelles.

Les administrateurs des systèmes d'information peuvent prendre connaissance de ces contenus privés en cas de nécessité avérée relative à la continuité du service, à la sécurité, à la maintenance des systèmes d'information ou bien en cas d'obligation légale.

L'utilisateur a une obligation de réserve et de confidentialité à l'égard des informations et documents qu'il produit ou auxquels il accède. Il n'accède qu'aux informations en rapport avec sa fonction. En particulier il ne cherche pas à accéder sans autorisation à des informations confidentielles ou sensibles. Il ne cherche pas à accéder sans autorisation à des systèmes d'information à régime restrictif ou à des zones à régime restrictif (ZRR) tels que définis par le dispositif de protection du potentiel scientifique et technique de la nation (PPST).

Il n'exploite pas des informations professionnelles à des fins non professionnelles.

VI.2 Données confidentielles et sensibles

Une information est considérée comme confidentielle pour un utilisateur ou pour un tiers lorsqu'il n'est pas autorisée à la connaître.

Doivent être considérées comme sensibles, certaines données personnelles, les données de santé, des informations à régime restrictif telles que définies par le dispositif de protection du potentiel scientifique et technique de la nation (PPST), des informations techniques (configuration des équipements, cartographie des éléments de sécurité informatique...).

L'information peut cesser d'être sensible après une période donnée, par exemple, une fois qu'elle a été rendue publique.

L'utilisateur ne communique les informations confidentielles ou sensibles qu'aux personnes dûment habilitées. Avant tout envoi, il est impératif de bien vérifier l'identité des destinataires du message et leur qualité à recevoir ces informations.

Les courriers électroniques n'étant pas sécurisés par défaut, les utilisateurs doivent limiter l'envoi d'informations à caractère confidentiel ou sensible aux nécessités de leurs missions professionnelles, et d'autant plus pour les messages externes. En cas de besoin, un chiffrement des messages et/ou des pièces jointes pourra être proposé par la DSI.

Les postes contenant des données sensibles doivent être chiffrés.

VI.3 Zones à régime restrictif « ZRR »

Les zones à régime restrictif (ZRR) sont encadrées par le fonctionnaire de sécurité défense de l'Université, qui agit de concert avec le RSSI de l'Université pour les questions de sécurité informatique.

Les ZRR bâtementaires se déclinent aux niveaux des services numériques utilisés dans ce cadre, des données produites et des systèmes informatiques sous-jacents.

La présente charte s'applique sans préjudice des règles spécifiques applicables au sein des ZRR.

Les utilisateurs de services numériques « ZRR » et « hors ZRR » doivent apporter un soin particulier aux transferts de données entre services numériques. Il est en particulier a priori interdit de transférer des données d'un services numérique « ZRR » vers un service numérique « hors ZRR ».

VI.4 Données à caractère personnel

Les utilisateurs respectent les dispositions légales en matière de traitements automatisés ou manuels de données à caractère personnel, conformément au Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (**RGPD**) et à la loi numéro 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite loi *Informatique et libertés* modifiée et à tout texte qui viendrait s'y substituer ou y apporter des modifications.

L'Université met en œuvre les moyens humains et organisationnels propres à assurer le respect desdites dispositions.

Tout traitement de données à caractère personnel doit être conforme aux textes susvisés. Un traitement s'entend de toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction. Cette disposition s'entend que le support soit numérique ou papier et s'étend aux systèmes de contrôle (dont la vidéosurveillance).

Tout utilisateur souhaitant procéder à un traitement de données à caractère personnel dans le cadre de son exercice professionnel est tenu d'en informer, préalablement à tout traitement et dès la conception du projet donnant lieu au traitement, le délégué à la protection des données (DPO) à

l'adresse dpo@u-bordeaux.fr. Ce dernier prendra les mesures nécessaires au respect des dispositions légales.

Les modalités de protection des données à caractère personnel, ainsi que celles relatives au droit d'accès permanent, de modification, de rectification et d'opposition dont dispose toute personne concernée, s'agissant des informations la concernant, seront consultables dans les *Politiques de confidentialité*, sur le site de l'Université. Un espace dédié aux données à caractère personnel sera ouvert à tout utilisateur sur le même site.

VII. Communication numérique

L'utilisation des moyens de communication numériques (messagerie, réseaux sociaux, blogs, etc.) est soumise aux recommandations de la *Charte du bon usage du numérique pour améliorer la qualité de vie au travail de tous* ou à tout document qui viendrait à s'y substituer.

L'utilisateur qui utilise le système d'information de l'Université pour contribuer à des forums de discussion, systèmes de discussion instantanée, blogs, sites, etc. veille à ne pas porter atteinte à l'image de l'Université.

Les échanges respectent les règles de correction, de décence, de réserve et de bienveillance d'usage dans toute correspondance. Ils respectent les règles édictées par la section IV. 4.

VII.1 Messagerie électronique

L'Université de Bordeaux met à la disposition de l'utilisateur une messagerie électronique nominative lui permettant d'émettre et de recevoir des messages électroniques à caractère professionnel.

Afin d'assurer la sécurité et la confidentialité des messages, pièces et documents joints, l'utilisateur s'oblige à utiliser la messagerie mise à sa disposition par l'Université et s'interdit, pour un usage professionnel, d'utiliser son adresse mail personnelle ou de recourir au service d'un prestataire tiers fournissant un service de messagerie.

La messagerie électronique peut constituer le support d'une communication privée dans les limites définies à la section IV. Tout message est réputé professionnel à moins que son objet ne commence par le mot *privé*.

VII.2 Adresse électronique

La gestion d'adresses électroniques correspondant à des listes de diffusion institutionnelles et désignant des groupes d'utilisateurs est de la responsabilité exclusive de l'Université. L'utilisation de ces adresses est soumise à l'autorisation de la Présidence ou de la Direction générale des services de l'Université. L'utilisateur est particulièrement attentif au contenu, au volume, à la fréquence, à la pertinence et aux conséquences des messages qu'il adresse à ces listes de diffusion.

VII.3 Contenu des messages

Un message électronique a la même portée qu'un courrier manuscrit. Il engage les responsabilités civile et pénale de l'Université et celles de l'utilisateur. Il est un document administratif reconnu comme preuve en cas de contentieux. Il est susceptible de former un contrat sous réserve du respect des conditions fixées par les articles 1369-1 à 1369-11 du code civil. L'utilisateur doit donc se montrer attentif au contenu des messages qu'il échange.

VII.4 Emission et réception des messages

Pour garantir la pertinence et la confidentialité des données l'utilisateur doit vérifier l'identité et les adresses de tous les destinataires et s'assurer qu'ils sont tous concernés par le contenu du message.

La même vigilance s'impose dans l'usage de tous les espaces collaboratifs (répertoires partagés, intranet, etc.)

Afin de limiter l'utilisation de la messagerie électronique en tant que vecteur de propagation des attaques cyber, des limitations et une surveillance sont opérées sur les flux de messagerie électronique. Le nombre de messages qu'un utilisateur est autorisé à envoyer sur une période de temps donnée est limité et la détection d'une suspicion d'utilisation d'une identité numérique IDNUM usurpée à des fins de propagation de cyberattaque conduit à la suspension préventive et sans délai de l'IDNUM concernée.

VII.5 Stockage et archivage des messages

L'Université sauvegarde quotidiennement les boîtes de messagerie des utilisateurs et conserve les sauvegardes sur une durée glissante de 30 jours.

L'utilisateur purge régulièrement sa boîte de messagerie et assure lui-même, par un archivage personnel, la conservation des messages, pièces et documents joints, utiles à son travail ou susceptibles de constituer des preuves. Il détermine les critères de conservation ainsi que la méthode et la durée adaptées de ce stockage, dans le respect de la réglementation applicable en matière d'archives.

VII.6 Sécurité de la messagerie

Des campagnes d'hameçonnage ou de courriels frauduleux ciblent l'université de Bordeaux. L'objectif est de vous diriger vers des sites web malveillants ou de récupérer des informations confidentielles (identifiants et mots de passe, informations bancaires...) qui peuvent produire de graves dommages aux systèmes d'information de l'Université ou vous porter directement préjudice (usurpation d'identité, compte bloqué...). L'utilisateur doit être particulièrement vigilant et respecter impérativement quelques règles de base :

- Si un message paraît suspect, même s'il émane d'un expéditeur connu, examiner attentivement le message, l'adresse mail complète de l'expéditeur et l'objet du courriel avant de l'ouvrir et plus encore avant d'ouvrir les pièces jointes ou de suivre des liens contenus dans le message
- Se méfier des courriels signalant des mises à jour systèmes, de maintenance ou contenant un message alarmant ou menaçant et demandant de cliquer sur un lien
- Ne pas ouvrir les messages suspects ni leurs pièces jointes, les classer dans le dossier « Spam » et vider le dossier
- Changer immédiatement le mot de passe si l'utilisateur a cliqué sur un lien frauduleux

Des tests peuvent être réalisés par l'Université afin de vérifier la vigilance et le besoin d'accompagnement des utilisateurs comme par exemple une campagne de test d'hameçonnage.

VIII. Protection des mineurs

Dans le cadre de ses activités, l'Université est susceptible d'accueillir des mineurs (stagiaires de l'enseignement secondaire notamment) dans ses locaux. Il incombe aux utilisateurs accueillant ces mineurs de les protéger en les préparant, en les conseillant, en les assistant notamment dans leur utilisation de l'Internet et des services numériques ainsi que de leur communiquer la charte en vigueur.

L'ensemble des activités liées aux technologies de l'information et de la communication, effectuées dans l'enceinte de l'Université et mettant en œuvre les services proposés doivent être précédées d'explications ou d'instructions très précises données aux mineurs. Celles-ci doivent notamment porter sur les conditions visées dans cette charte et, le cas échéant, insister sur des consignes spécifiques de sécurité.

Les utilisateurs doivent garder à tout moment, la maîtrise des activités liées à l'utilisation des services proposés par l'Université, notamment en exerçant une surveillance suivie des activités des mineurs, de manière à pouvoir intervenir rapidement en cas de problème, à repérer et faire cesser tout comportement pouvant devenir dangereux.

IX. Propriété intellectuelle

L'utilisateur des moyens d'information et de communication de l'Université est tenu au respect des droits de propriété intellectuelle, ceux de l'Université comme ceux des tiers. Il doit notamment :

- ne pas utiliser, représenter, reproduire, copier, diffuser, modifier les œuvres (photographies, textes, dessins etc) protégées par des droits de propriété intellectuelle sans avoir préalablement obtenu l'autorisation du ou des titulaires de ces droits ;
- n'utiliser les logiciels, bases de données, textes, images ou toutes autres créations que dans le strict respect des licences souscrites.

Pour rappel, l'utilisation d'un œuvre de l'esprit sans l'autorisation préalable et écrite de son auteur ou des titulaires des droits est constitutif d'une contrefaçon.

Quelques textes de référence applicables

1./ Sanctions pénales encourues en cas d'atteinte aux systèmes automatisés de données

Articles 323-1 à 323-7 du code pénal

2./ Sanctions disciplinaires encourues par les usagers

Articles 811-10 à 811-42 du code de l'éducation

3./ Sanctions disciplinaires encourues par les enseignants-chercheurs et membres des corps des personnels enseignants de l'enseignement supérieur

Article 952-8 du code de l'éducation

4./ Sanctions disciplinaires encourues par les autres enseignants en cas d'infraction

Article 952-9 du code de l'éducation

5./ Sanctions disciplinaires encourues par les personnels ingénieurs, administratifs, techniques, ouvriers et de service titulaires

Article 66 de la loi numéro 84-16 du 11 janvier 1984

6./ Sanctions disciplinaires encourues par les agents contractuels

Article 43-2 du décret numéro 86-83 du 17 janvier 1986

7./ Protection du potentiel scientifique et technique de la nation (PPST)

Articles 413-1 à 413-8 du code pénal

Décret numéro 2011-1425 du 2 novembre 2011

Arrêté du 3 juillet 2012 relatif à la protection du potentiel scientifique et technique de la
Circulaire interministérielle numéro 3415/SGDSN/AIST/PST du 7 novembre 2012 de mise

8./ Droit de la propriété intellectuelle

Le code de la propriété intellectuelle

Et en particulier :

Article L112 : Les œuvres de l'esprit concernées par le droit d'auteur

Article L122-5 : Les exceptions

Article L335 : Le délit de contrefaçon

9./ Protection des données à caractère personnel

Loi numéro 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés

Règlement (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

Articles 226-16 à 226-24 du code pénal

Articles R625-10 à R625-13 du code pénal pour les sanctions encourues.

10./ Atteinte à la vie privée

Article 9 du code civil

Articles 226-1 à 226-7 du code pénal

11./ Atteinte à la représentation de la personne

Articles 226-8 à 226-9 du code pénal

12./ Obligation de conservation des données d'identification

Loi pour la confiance numérique du 21 juin 2004, article 6-II

Code des postes et des communications électroniques, article L34-1