Projet : **sécurité du système d'information**	Date : **26 mars 2021**
Type : **charte administrateur**	Version — Révision : **1.00**

CHARTE ADMINISTRATEUR DE L'UNIVERSITE BORDEAUX MONTAIGNE

ADOPTEE PAR LE CONSEIL D'ADMINISTRATION DU 26 MARS 2021

Référence **:**
Charte_administrateur_Bordeaux_Montaigne_V1.0 Numéro de la dernière page : **13**
0.docx

DIFFUSION :	☐Publique	☐Restreinte	☑Confidentielle

SOMMAIRE

PREAMBULE 3

1 PORTEE ET OPPOSABILITE 3

2 CHAMP D'APPLICATION ET RESPECT DE LA CHARTE 3

3 DEFINITIONS 3

4 ADMINISTRATEUR D'UN SYSTEME D'INFORMATION 4

4.1 IDENTIFICATION DES ADMINISTRATEURS D'UN SYSTEME D'INFORMATION 4
4.2 ATTENDUS DE LA FONCTION 4
4.3 RELATION AVEC LES UTILISATEURS 5
4.4 DROITS DE L'ADMINISTRATEUR 6
4.5 DEVOIRS DE L'ADMINISTRATEUR 6
4.6 TRAITEMENT DES DYSFONCTIONNEMENTS ET DES INCIDENTS DE SECURITE 7

5 ENGAGEMENT INDIVIDUEL DE RESPONSABILITE 8

ANNEXE 1.1 – EXEMPLAIRE CONSERVE PAR L'ADMINISTRATEUR 9

ANNEXE 1.2 – EXEMPLAIRE CONSERVE PAR LA DSIN 11

ANNEXE 2 - PRINCIPALES REFERENCES LEGISLATIVES 13

INFRACTIONS PREVUES PAR LE NOUVEAU CODE PENAL 13
INFRACTIONS DE PRESSE (LOI 29 JUILLET 1881, MODIFIEE) 13
INFRACTION AU CODE DE LA PROPRIETE INTELLECTUELLE 13
PARTICIPATION A LA TENUE D'UNE MAISON DE JEUX DE HASARD (« CYBER-CASINO ») 13

PREAMBULE

À l'heure où les systèmes d'information, de communication et les services numériques sont de plus en plus interconnectés et les réseaux de plus en plus imbriqués, la transformation numérique est à la fois marqueur de progrès et catalyseur de risques. Si les bénéfices apportés par le numérique ne sont plus à prouver, la fiabilité de ces derniers sera garantie à la seule condition que les systèmes soient sécurisés et que les données soient protégées.

Du fait de leurs activités et des droits étendus dont ils disposent au sein du système d'information de l'Université Bordeaux Montaigne, les administrateurs sont un maillon des plus sensibles de la protection des informations de l'université.

Ces administrateurs peuvent effectuer des actions sensibles tels que des modifications de configurations, de dispositifs de protection et de détection, de droits d'accès, etc. Ces actions sont de nature à toucher aux besoins de sécurité des informations et des systèmes les hébergeant, tels que leur disponibilité, leur intégrité ou leur confidentialité.

De ce fait, les administrateurs ont un rôle essentiel nécessitant l'exemplarité. Conformément aux obligations statutaires propres à tout agent public, et notamment celles liées aux devoirs de réserve, loyauté, probité, secret et discrétion professionnels, l'intervention des administrateurs ne doit pas outrepasser leurs attributions ni relever d'actions effectuées pour leur propre compte ou par intérêt personnel. Ils doivent également être protégés des pressions ou des attaques qui pourraient s'exercer à leur encontre afin d'exploiter les accès dont ils bénéficient.

Prenant en compte les préconisations de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), de la Commission nationale de l'informatique et des libertés (CNIL), la présente charte précise le cadre légal, réglementaire et déontologique dans lequel doivent s'inscrire les actions d'administration des systèmes d'information. Elle complète la **charte régissant l'usage du système d'information de l'université Bordeaux Montaigne** adoptée par le Conseil d'Administration du 26 mars 2021. Cette charte s'inscrit dans les politiques de Sécurité du Système d'Information de l'Université Bordeaux Montaigne.

1 PORTEE ET OPPOSABILITE

La présente charte et les modifications ultérieures qui pourraient intervenir sont applicables dès son approbation par le conseil d'administration de l'université. En conséquence, elle est opposable à l'Administrateur (cf. § Définitions) des services numériques (cf. § Définitions) et il est supposé en avoir pris connaissance. La signature de l'engagement individuel de responsabilité en annexe de cette charte atteste de la prise de connaissance par l'administrateur.

Aucune clause dudit document n'a pour but de déroger aux accords collectifs ou d'entreprise, ou aux droits des représentants du personnel et des sections syndicales de l'université, ni d'apporter aux droits des personnes et aux libertés individuelles et collectives des restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché conformément à la législation en vigueur.

2 CHAMP D'APPLICATION ET RESPECT DE LA CHARTE

L'objet de la présente charte est d'informer les administrateurs des services numériques de l'Université Bordeaux Montaigne de leurs droits et obligations.

Les administrateurs des systèmes d'information s'engagent à respecter en toute circonstance la réglementation en vigueur, ainsi que la présente charte et la charte régissant l'usage du système d'information de l'Université Bordeaux Montaigne. En cas de non-respect des textes en vigueur ou des dispositions de la présente charte, l'administrateur sera tenu pour responsable de ses actes et encourra les sanctions pénales, civiles, administratives et disciplinaires prévues par les textes applicables.

Tout document relatif aux règles, procédures, conditions ou missions d'administration d'un système d'information doit être conforme aux principes de la présente charte.

3 DEFINITIONS

Les définitions suivantes s'appliquent dans la suite du document :

- **Administrateur** : toute personne (ou groupe de personnes) chargée(s) de l'exploitation, de la maintenance et de la supervision d'un service numérique, ou d'une partie de ce dernier. Il s'agit notamment de :
  - tout agent titulaire ou non titulaire de l'université concourant au travers de ces tâches d'administration à l'exécution des missions du service numérique de l'université ;

- tout consultant ou prestataire ayant contracté avec l'université et intervenant sur des fonctions d'exploitation, de maintenance et de supervision d'un service numérique de l'université.

- **Propriétaire :** se comprend en termes de responsabilités, et non au sens de propriété juridique. Les directeurs ainsi que leurs chefs de service sont propriétaires de leurs données métier.
- **Système d'information** : ensemble des ressources matérielles, logicielles, applications, bases de données et réseaux de télécommunications, pouvant être mis à disposition par l'université. Il est aussi constitué des dispositifs numériques nomades personnels connectés au réseau de l'Université. Ainsi, les micro-ordinateurs fixes ou portables, les moyens de communication (messagerie, accès à l'Internet, réseaux de transmission voix ou données, téléphones fixes ou portables, télécopieurs, service de visio-conférence, etc.), les équipements de stockage de données (disques durs externes, clés USB, supports optiques tel que le DVD etc.), les données contenues sur les équipements précédemment cités, les applications informatiques et autres logiciels font partie du système d'information de l'Université Bordeaux Montaigne.
- **Université** : L'Université Bordeaux Montaigne.

4 ADMINISTRATEUR D'UN SYSTEME D'INFORMATION

4.1 Identification des administrateurs d'un système d'information

La Direction des Services Informatiques et Numériques (DSIN) tiens à jour la liste des administrateurs du système d'information.

Sur les périmètres du système d'information de l'université non administrés par la DSIN, les propriétaires des actifs tiennent à jour, sur le périmètre de leur responsabilité, la liste des profils administrateurs et des services qui leurs sont associés, en précisant la nature et le périmètre de leurs droits. Cette liste est communiquée à la DSIN qui en assure le contrôle.

Lorsqu'il s'agit de personnels de prestataires extérieurs, ces éléments sont précisés dans le contrat.

Les listes des profils d'accès et des identités des différents administrateurs sont communiquées, à sa demande, au responsable de la sécurité des systèmes d'information (RSSI) de l'université.

4.2 Attendus de la fonction

4.2.1 Compétences

L'université s'assure que l'administrateur dispose des compétences requises par la fonction dans les domaines :

- techniques relatifs aux ressources matérielles et logicielles gérées ;
- des lois et règlements applicables au système d'information administré, leurs évolutions et, plus généralement, le domaine juridique des nouvelles technologies ;
- de la politique de sécurité des systèmes d'information de l'université ;
- de l'application à ces systèmes des mesures de sécurité et des mesures d'urgence ;
- du suivi des vulnérabilités du (des) système(s) servi(s), des menaces pesant sur eux et des méthodes d'attaques de ces systèmes ;
- du suivi du niveau d'alerte SSI et de l'actualité de la menace.

L'université évalue les besoins en formation des administrateurs et veille au maintien de leurs compétences.

L'administrateur met en œuvre la politique de sécurité de l'information de l'université. Il déploie les mesures qui s'imposent sur son périmètre. Il informe le RSSI de tout incident de sécurité dès sa constatation.

4.2.2 Principe de maitrise des droits d'administration

L'Université privilégie les comptes d'accès individuels pourvus des privilèges d'administration. Les comptes d'accès génériques tels que **root** ou **administrateur** ne sont utilisés qu'en dernier recours, les authentifications par clés individuelles sont alors privilégiées.

Lorsque l'authentification est réalisée au moyen d'un mot de passe celui-ci doit être suffisamment long et complexe (au moins 20 caractères). Il doit être changé régulièrement selon un rythme propre à ne pas gêner l'administration, conformément aux préconisations de la politique de sécurité.

4.2.3 Principe du moindre privilège

L'administrateur ne peut faire usage de ses droits à d'autres fins que celles de sa mission et sur le périmètre qui lui est dévolu. Il s'interdit tout accès à toute information hors du champ de sa mission d'administration. Il ne modifie les configurations et les droits d'accès que dans le respect de procédures d'administration ou d'exploitation définies.

Pour toute autre tâche que celle d'administration et plus généralement lorsque l'utilisation de droits particuliers n'est pas nécessaire, l'administrateur s'identifie sur le système d'information avec un profil n'en comportant pas.

Afin d'assurer la sécurité des opérations d'administration, l'administrateur veille au bon niveau de sécurité du poste à partir duquel ces opérations sont effectuées. Il s'assure notamment de ne pas être administrateur de son poste lors de ces opérations.

4.2.4 Continuité de l'activité

Les opérations d'administration doivent être conduites de manière à maintenir la continuité du service rendu aux utilisateurs.

L'administrateur effectue ces opérations dans le respect des procédures de planification ou d'exploitation définies. Il recueille l'autorisation de sa hiérarchie et s'assure de l'application de la procédure d'information des utilisateurs et services.

Dans tous les cas, si l'administrateur doit interrompre tout ou partie du service rendu aux utilisateurs, il choisit des plages horaires minimisant la gêne occasionnée et réduit autant que possible la durée et la fréquence des interruptions en accord avec sa hiérarchie.

4.2.5 Secret Professionnel

Les administrateurs, en tant que dépositaires de renseignements concernant ou intéressant des particuliers, sont tenus au secret professionnel dans le cadre des règles instituées par le Code pénal.

L'obligation n'est cependant pas absolue. La révélation des secrets acquis est requise ou permise lorsque les nécessités du service ou des obligations légales l'imposent et notamment :

- pour prouver son innocence ;
- lorsque la personne intéressée a donné son autorisation.

Elle est obligatoire notamment dans les cas suivants :

- dénonciation de crimes ou délits dont un fonctionnaire a connaissance dans l'exercice de ses fonctions ;
- communication de renseignements, pièces et documents aux autorités de justice agissant en matière criminelle ou correctionnelle ;
- témoignage en justice en matière criminelle ou correctionnelle ;
- communication des pièces et documents nécessaires au juge administratif saisi d'un recours contre un acte administratif ou au juge judiciaire saisi d'un litige.

4.2.6 Discrétion professionnelle

Comme tout fonctionnaire ou assimilé, l'administrateur doit faire preuve de discrétion professionnelle pour tous les faits, informations ou documents dont il a connaissance dans l'exercice ou à l'occasion de l'exercice de sa fonction.

Cette obligation est instituée, dans l'intérêt du service, pour protéger les informations de l'université dont la divulgation pourrait nuire au bon fonctionnement de ses tâches. Le non-respect de cette obligation, hormis dans les cas expressément prévus par la loi ou sous couvert de l'autorité dont dépend l'utilisateur, l'expose à des sanctions disciplinaires.

L'administrateur fait preuve de prudence lors des échanges qu'il peut être amené à avoir sur les réseaux d'entraide ou tout document accessible à un large public afin de ne pas dévoiler des éléments techniques ou organisationnels qui pourraient être utilisés à l'encontre de l'institution.

4.3 Relation avec les utilisateurs

Les règles et procédures d'administration des systèmes d'information et de sécurité servent en priorité à la mise en œuvre, au maintien ou à l'amélioration de la qualité des prestations délivrées à l'utilisateur.

L'administrateur s'assure de la qualité du service rendu aux utilisateurs et contribue à leur soutien en liaison avec les autres intervenants, notamment par le transfert d'un minimum d'informations permettant aux utilisateurs de bénéficier du système en condition normale et de faire appel, le cas échéant, à une assistance.

L'administrateur participe également à la sensibilisation des utilisateurs :

- en rappelant régulièrement les principes de la charte d'usage du système d'information ;
- en informant les utilisateurs des consignes techniques de sécurité à mettre en œuvre afin de préserver le système d'information ;
- en participant à la sensibilisation des utilisateurs aux usages raisonnés du numérique et aux risques encourus par l'université et eux-mêmes ;
- chaque fois que cela est possible, les administrateurs invitent l'utilisateur à séparer ses documents privés de ses documents professionnels et à les mettre dans un répertoire portant la mention « PRIVE » ou « privé » afin de faciliter le respect de l'intimité de sa vie privée.

4.4 Droits de l'administrateur

L'administrateur est informé par sa hiérarchie des implications légales de son travail et ne peut être contraint à enfreindre la loi.

Il bénéficie d'une protection juridique vis à vis du refus d'obéir aux actions manifestement illégales commandées par sa hiérarchie ou de nature à compromettre gravement un intérêt public.

Actions autorisées de l'administrateur sur son périmètre

Dans le cadre du respect de la politique de sécurité du système d'information (PSSI) l'administrateur peut :

- mettre en place des moyens permettant de fournir des informations techniques d'administration de réseau ;
- mettre en place toutes procédures appropriées pour vérifier la bonne application des règles de contrôle d'accès aux systèmes et aux réseaux définies dans la Politique de Sécurité du Système d'Information, en utilisant des outils autorisés ;
- accéder, sur les systèmes qu'il administre, à tout type d'information, mais uniquement à des fins de diagnostic et d'administration du système, en respectant scrupuleusement la confidentialité de ces informations, en s'efforçant - tant que la situation ne l'exige pas - de ne pas les altérer ;
- établir des procédures de surveillance de toutes les tâches exécutées sur le matériel informatique utilisé, afin de déceler les violations ou les tentatives de violation de la présente charte et de la charte d'usage du système d'information, sous l'autorité de son responsable et en relation avec le RSSI.

Dans les cas où le maintien en condition de sécurité du système d'information considéré l'exige, l'accès aux dossiers ou mails revêtant la mention « PRIVE » ou « privé » peut être opéré par les outils automatiques (ex. : antivirus) ou les administrateurs eux-mêmes.

Dans ce cas, l'accès aux dossiers ou courriels personnels de l'utilisateur par l'administrateur doit se faire en présence de l'utilisateur, sauf cas de force majeure. En tout état cause, tous les moyens nécessaires doivent être mis en œuvre pour informer l'utilisateur préalablement à l'intervention de l'administrateur. Cette intervention n'autorise en aucune manière l'administrateur à révéler à quiconque le contenu des fichiers personnels, en dehors des exceptions et limites légales sus rappelées.

4.5 Devoirs de l'administrateur

L'administrateur doit :

- respecter les dispositions légales et réglementaires concernant le système d'information. Le doute entraîne la consultation du RSSI ou de la cellule juridique de l'Université ;
- se conformer à la politique de sécurité des systèmes d'information de l'établissement, appliquer les procédures d'exploitation de sécurité attachées aux systèmes d'information dont il a la charge et rendre compte de toute difficulté d'application. À défaut de procédures formalisées, il applique les règles générales de sécurité correspondant à l'environnement d'exploitation prescrit ;
- respecter la confidentialité des informations auxquelles il accède lors de ses tâches d'administration quel qu'en soit le support et la nature ;

- n'effectuer des accès aux contenus marqués comme « PRIVE » ou « privé » qu'en présence de l'utilisateur ou avec son autorisation écrite, à l'exception des cas d'atteinte à la sécurité sous couvert d'autorisation du RSSI ou de l'utilisation d'outils automatiques, tels qu'antivirus ou inventaire logiciel, qui ne visent pas individuellement l'utilisateur ;
- garantir la transparence dans l'emploi d'outils de prise en main à distance ou toute autre intervention sur l'environnement de travail individuel de l'utilisateur ;
- s'assurer de l'identité et de l'habilitation de l'utilisateur lors de la remise de tout élément du système d'information en collaboration avec le responsable fonctionnel ;
- répondre à toute consigne de surveillance, de recueil d'information ou d'audit émise par le RSSI.

En cas d'incident l'administrateur doit :

- le traiter en première priorité et prendre toute disposition nécessaire pour toute violation des règles de sécurité et tout incident de sécurité qu'il est amené à constater et en informer sans délai le RSSI ;
- prendre des mesures conservatoires si l'urgence l'impose.

Les principales actions d'administration sont consignées soit de manière automatique, soit de manière manuelle, afin que le cours des événements puisse être au besoin fidèlement retracé. L'administrateur tient en outre à jour la documentation technique et les configurations de tous les composants du système d'information. L'administrateur veille à ne pas porter atteinte à l'intégrité des fichiers de journalisation et ne désactive pas les mécanismes de traçabilité. En cas de force majeure seul le RSSI peut prendre l'initiative d'une désactivation temporaire.

L'administrateur veille à ce que les logiciels soient utilisés dans les conditions de licences souscrites. Dans le cadre de sa mission, il n'utilise que des logiciels conformes à la politique de sécurité de l'université. Toute dérogation doit faire l'objet d'une autorisation préalable et explicite de son responsable hiérarchique et du RSSI.

En cas de requête officielle des autorités judiciaires, l'administrateur remet toute information demandée, en lien avec son responsable hiérarchique.

Les informations issues des dispositifs dédiés à la capture et/ou l'enregistrement d'images ou de conversations à des fins de surveillance, de preuve, de formation ou d'évaluation ne doivent être consultées que par le personnel habilité, formé et investi d'une mission de surveillance ou de contrôle, ce qui exclut le personnel administrateur.

Si un administrateur venait exceptionnellement à prendre connaissance du contenu des enregistrements pour des motifs légitimes de maintien en condition de sécurité du système, les principes exposés précédemment lui interdisent de divulguer les informations dont il aurait ainsi eu connaissance.

4.6 Traitement des dysfonctionnements et des incidents de sécurité

4.6.1 Généralités

Dans le cadre de ses fonctions, l'administrateur peut être alerté sur des dysfonctionnements ou des incidents de sécurité touchant le système d'information :

- sont appelées dysfonctionnements toutes les défaillances physiques ou logiques rencontrées sur le système, voire sur les servitudes indispensables à son bon fonctionnement. L'administrateur réagit alors selon les consignes propres au système concerné ;
- sont appelés incidents de sécurité tous les faits ou événements volontaires ou involontaires, issus d'un utilisateur légitime ou non, voire d'un système externe, et portant atteinte à la sécurité du système administré ou au respect de la loi.

Un administrateur constatant un incident de sécurité doit prendre immédiatement les mesures permettant :

- de faire cesser l'incident en cours et de se préserver d'éventuels effets ultérieurs selon les procédures mises en place et en cohérence avec le besoin opérationnel qui reste prioritaire ;
- de recouvrer le niveau de sécurité normal du système ;
- d'assurer la continuité de service, au besoin en mode dégradé.

Il rend compte sans délai à sa hiérarchie et au RSSI des faits constatés et des actions de remédiation conduites.

Certains incidents pouvant déboucher sur des poursuites disciplinaires ou judiciaires, l'administrateur prend les mesures adaptées afin de préserver les éléments de preuve de l'acte malveillant.

4.6.2 Préservation des preuves

La preuve est la démonstration de la réalité d'un fait, d'un état, d'une circonstance ou d'une obligation. Elle a pour finalité soit d'apporter des éléments contradictoires aux faits contestés, soit d'établir les allégations et ainsi d'aider le juge à se forger une intime conviction, ou l'autorité hiérarchique à apprécier l'opportunité d'une éventuelle sanction ou action en justice.

L'administrateur doit agir rapidement, et si possible en présence du RSSI (ou de l'un de ses suppléants en qualité de témoin, afin de fixer la preuve dans le temps et d'éviter sa disparition ou son altération. À ce titre, les actions suivantes sont à mener sans délai :

- déconnecter le serveur, le poste de travail ou l'élément de stockage du réseau afin d'éviter toute action d'effacement ou de modification de preuve postérieure à la découverte du délit. En fonction des besoins opérationnels, la continuité de service devra être assurée, le cas échéant, par la mise en oeuvre d'un mécanisme de secours ;
- éviter, dans la mesure du possible, d'éteindre l'équipement incriminé (cette opération pourrait avoir pour effet d'effacer les traces présentes en mémoire) ; si la machine doit cependant être éteinte, ne pas utiliser la fonction d'extinction du système mais débrancher le cordon d'alimentation ;
- verrouiller le(s) compte(s) du (des) utilisateur(s) incriminé(s), ainsi que l'accès aux comptes de messagerie ;
- ne pas connecter de supports amovibles sans nécessité afin de ne pas générer de traces parasites ;
- restreindre l'accès physique à l'élément incriminé de sorte que personne ne modifie sa configuration avant l'intervention des services compétents.
- noter, sur un journal de bord, l'ensemble des constatations faites et des actions effectuées de manière à assurer une traçabilité et un historique de l'incident en précisant :
    - les dates et heures du système ainsi que les dates et heures réelles, celles-ci pouvant différer ;
    - le nom des fichiers ou commandes exécutés ainsi que les identifiants et mots de passe utilisés si des actions d'administration sont nécessaires ;
- préserver le plus grand nombre d'informations pertinentes pouvant compléter les investigations tels que supports de sauvegardes récentes ou journaux d'évènements.
- Dans tous les cas, il y a lieu d'agir avec la plus grande discrétion et respecter le principe de la présomption d'innocence.

5 ENGAGEMENT INDIVIDUEL DE RESPONSABILITE

Chaque administrateur d'un système d'information est tenu de prendre connaissance de la charte et s'engage à la respecter par la signature d'un engagement individuel de responsabilité.

L'engagement individuel de responsabilité est signé en deux exemplaires par l'administrateur et cosigné par son supérieur hiérarchique. Un exemplaire est conservé par la DSIN et l'autre par l'administrateur lui-même.

Les principales dispositions légales et réglementaires en vigueur dans le domaine de la sécurité des systèmes d'information sont énumérées dans l'annexe juridique.

ANNEXE 1.1 – EXEMPLAIRE CONSERVE PAR L'ADMINISTRATEUR

ENGAGEMENT INDIVIDUEL DE RESPONSABILITÉ DE L'ADMINISTRATEUR DE SYSTÈME D'INFORMATION

Je soussigné/e Monsieur/Madame ....., exerçant les fonctions d'administrateur au sein de l'Université Bordeaux Montaigne, déclare avoir pris connaissance de la charte des administrateurs du système d'information de l'Université Bordeaux Montaigne et m'engage à la respecter et, étant au titre de mes fonctions amené/e à accéder à des données à caractère personnel, déclare reconnaître la confidentialité desdites données.

Je m'engage par conséquent, conformément aux articles 34 et 35 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ainsi qu'aux articles 32 à 35 du règlement général sur la protection des données du 27 avril 2016, à prendre toutes précautions conformes aux usages et à l'état de l'art dans le cadre de mes attributions afin de protéger la confidentialité des informations auxquelles j'ai accès, et en particulier d'empêcher qu'elles ne soient communiquées à des personnes non expressément autorisées à recevoir ces informations.

Je m'engage en particulier à :

- ne pas utiliser les données auxquelles je peux accéder à des fins autres que celles prévues par mes attributions ;
- ne divulguer ces données qu'aux personnes dûment autorisées, en raison de leurs fonctions, à en recevoir communication, qu'il s'agisse de personnes privées, publiques, physiques ou morales ;
- ne faire aucune copie de ces données sauf à ce que cela soit nécessaire à l'exécution de mes fonctions ;
- prendre toutes les mesures conformes aux usages et à l'état de l'art dans le cadre de mes attributions afin d'éviter l'utilisation détournée ou frauduleuse de ces données ;- prendre toutes précautions conformes aux usages et à l'état de l'art pour préserver la sécurité physique et logique de ces données ;
- m'assurer, dans la limite de mes attributions, que seuls des moyens de communication sécurisés seront utilisés pour transférer ces données ;- en cas de cessation de mes fonctions, restituer intégralement les données, fichiers informatiques et tout support d'information relatif à ces données.

Cet engagement de confidentialité, en vigueur pendant toute la durée de mes fonctions, demeurera effectif, sans limitation de durée après la cessation de mes fonctions, quelle qu'en soit la cause, dès lors que cet engagement concerne l'utilisation et la communication de données à caractère personnel.

J'ai été informé que toute violation du présent engagement m'expose à des sanctions disciplinaires et pénales conformément à la réglementation en vigueur, notamment au regard des articles 226-16 à 226-24 du code pénal.

Fait en deux exemplaires à ..... le .....

ENGAGEMENT DU SUPÉRIEUR HIÉRARCHIQUE DIRECT

Je soussigné, ... agissant en tant que supérieur hiérarchique direct de ..... déclare avoir pris connaissance de la charte des administrateurs du système d'information de l'Université Bordeaux Montaigne et m'engage à en respecter les termes et limites définies

Fait en deux exemplaires à ..... le .....

[page blanche]

ANNEXE 1.2 – EXEMPLAIRE CONSERVE PAR LA DSIN

ENGAGEMENT INDIVIDUEL DE RESPONSABILITÉ DE L'ADMINISTRATEUR DE SYSTÈME D'INFORMATION

Je soussigné/e Monsieur/Madame ....., exerçant les fonctions d'administrateur au sein de l'Université Bordeaux Montaigne, déclare avoir pris connaissance de la charte des administrateurs du système d'information de l'Université Bordeaux Montaigne et m'engage à la respecter et, étant au titre de mes fonctions amené/e à accéder à des données à caractère personnel, déclare reconnaître la confidentialité desdites données.

Je m'engage par conséquent, conformément aux articles 34 et 35 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ainsi qu'aux articles 32 à 35 du règlement général sur la protection des données du 27 avril 2016, à prendre toutes précautions conformes aux usages et à l'état de l'art dans le cadre de mes attributions afin de protéger la confidentialité des informations auxquelles j'ai accès, et en particulier d'empêcher qu'elles ne soient communiquées à des personnes non expressément autorisées à recevoir ces informations.

Je m'engage en particulier à :

- ne pas utiliser les données auxquelles je peux accéder à des fins autres que celles prévues par mes attributions ;
- ne divulguer ces données qu'aux personnes dûment autorisées, en raison de leurs fonctions, à en recevoir communication, qu'il s'agisse de personnes privées, publiques, physiques ou morales ;
- ne faire aucune copie de ces données sauf à ce que cela soit nécessaire à l'exécution de mes fonctions ;
- prendre toutes les mesures conformes aux usages et à l'état de l'art dans le cadre de mes attributions afin d'éviter l'utilisation détournée ou frauduleuse de ces données ;- prendre toutes précautions conformes aux usages et à l'état de l'art pour préserver la sécurité physique et logique de ces données ;
- m'assurer, dans la limite de mes attributions, que seuls des moyens de communication sécurisés seront utilisés pour transférer ces données ;- en cas de cessation de mes fonctions, restituer intégralement les données, fichiers informatiques et tout support d'information relatif à ces données.

Cet engagement de confidentialité, en vigueur pendant toute la durée de mes fonctions, demeurera effectif, sans limitation de durée après la cessation de mes fonctions, quelle qu'en soit la cause, dès lors que cet engagement concerne l'utilisation et la communication de données à caractère personnel.

J'ai été informé que toute violation du présent engagement m'expose à des sanctions disciplinaires et pénales conformément à la réglementation en vigueur, notamment au regard des articles 226-16 à 226-24 du code pénal.

Fait en deux exemplaires à ..... le .....

ENGAGEMENT DU SUPÉRIEUR HIÉRARCHIQUE DIRECT

Je soussigné, ... agissant en tant que supérieur hiérarchique direct de ..... déclare avoir pris connaissance de la charte des administrateurs du système d'information de l'Université Bordeaux Montaigne et m'engage à en respecter les termes et limites définies

Fait en deux exemplaires à ..... le .....

[page blanche]

ANNEXE 2 - PRINCIPALES REFERENCES LEGISLATIVES

Infractions prévues par le Nouveau Code pénal

Crimes et délits contre les personnes

Atteintes à la personnalité : (Respect de la vie privée art. 9 du code civil)

- Atteintes à la vie privée (art. 226-1 al. 2 ; 226-2 al. 2, art.432-9 modifié par la loi nº2004-669 du 9 juillet 2004) ;
- Atteintes à la représentation de la personne (art. 226-8)
- Dénonciation calomnieuse (art. 226-10)
- Atteinte au secret professionnel (art. 226-13)
- Atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques (art. 226-16 à 226-24, issus de la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

Atteintes aux mineurs : (art. 227-23 ; 227-24 et 227-28).

- Loi 2004- 575 du 21 juin 2004 (LCEN)

Crimes et délits contre les biens

- Escroquerie (art. 313-1 et suite)
- Atteintes aux systèmes de traitement automatisé de données (art. 323-1 à 323-7 modifiés par les lois nº 2004-575 du 21 juin 2004 et n°2015-912 du 24 juillet 2015).

Cryptologie

- Art. 132-79 (inséré par loi nº 2004-575 du 21 juin 2004 art. 37)

Infractions de presse (loi 29 juillet 1881, modifiée)

- Provocation aux crimes et délits (art.23 et 24)
- Apologie des crimes contre l'humanité, apologie et provocation au terrorisme, provocation à la haine raciale, « négationnisme » contestation des crimes contre l'humanité (art. 24 et 24 bis)
- Diffamation et injure (art. 30 à 33)

Infraction au Code de la propriété intellectuelle

- Contrefaçon d'une œuvre de l'esprit (y compris d'un logiciel) (art. 335-2 modifié par la loi nº 2004-204 du 9 mars 2004, art. 34 - et art. 335-3)
- Contrefaçon d'un dessin ou d'un modèle (art. L521-4 modifiée par la loi nº 2004-204 du 9 mars 2004, art. 34)
- Contrefaçon de marque (art. L716-9 - modifié par la loi nº 2004-204 du 9 mars 2004, art.34 -et suivants)

Participation à la tenue d'une maison de jeux de hasard (« cyber-casino »)

- Art.1 de la loi du 12 juillet 1983, modifié par la loi du 16 décembre 1992

Cette liste n'est qu'indicative et la législation est susceptible d'évolution.