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

Charte régissant l'usage du système d'information de l'université Bordeaux Montaigne

Adoptée par le conseil d'administration du 26 mars 2021

Référence : **Charte_informatique_Bordeaux_Montaigne_V1.00.docx**	Numéro de la dernière page : **15**

DIFFUSION :	☑ **PUBLIQUE**	☐ **RESTREINTE**	☐ **CONFIDENTIELLE**

SOMMAIRE

Document
Approuvé par : Le conseil d'administration de l'université Bordeaux Montaigne

Etat du document	
Révision	*Désignation des modifications*
1.00	*Version initiale*

Conditions d'accès au document
Ce document est accessible sur le site institutionnel de l'université, le site étudiant et l'ENTP.

Préambule

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

Du fait de ses activités et de sa mission de service public, l'université Bordeaux Montaigne doit garantir un niveau de sécurité adapté aux informations qu'elle est amenée à traiter.

Prenant en compte les préconisations de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et de la Commission nationale de l'informatique et des libertés (CNIL), ce texte s'inscrit dans le cadre législatif et réglementaire en vigueur relatif à la protection des données à caractère personnel, à l'utilisation des logiciels, aux droits et obligations des utilisateurs des services numériques. Il s'inscrit dans les politiques de sécurité du système d'Information de l'université Bordeaux Montaigne.

Glossaire, sigles et abréviations

Terme	Définition
Cnil	Commission nationale informatique et libertés.
DPD	Délégué à la protection des données
DPO	Data Protection Officer : délégué à la protection des données
RSSI	Responsable sécurité des systèmes d'information
SSI	sécurité des systèmes d'information

Article 1. **Portée et opposabilité**

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'Utilisateur (cf. Article 3 Définitions) des services numériques et il est supposé en avoir pris connaissance.

Aucune clause dudit document n'a pour but de déroger aux statuts et règlement intérieur de l'université, 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.

Article 2. **Champ d'application**

L'objet de la présente charte est d'informer les Utilisateurs des services numériques de l'université Bordeaux Montaigne de leurs droits et obligations. Elle a été élaborée dans le souci de concilier les intérêts de l'université Bordeaux Montaigne avec ceux des Utilisateurs.

Elle décrit ainsi l'ensemble des règles générales et spécifiques que chaque Utilisateur doit respecter dans l'utilisation des ressources et services numériques de l'université Bordeaux Montaigne, de manière à éviter de porter atteinte à la sécurité de l'université Bordeaux Montaigne, à la sécurité publique ou à la sécurité des usagers.

Chaque Utilisateur doit être conscient de l'impact de son usage quotidien ou occasionnel sur la sécurité des services numériques. Il s'engage à accepter ce règlement dans tous ses éléments et à le respecter dans tous ses termes.

Dans le cas d'une UMR, celle-ci peut prévoir des restrictions d'accès spécifiques à son organisation. Les Utilisateurs de ces unités sont notamment également soumis au respect, quand elles existent, des politiques de sécurité du système d'information de l'unité édictées par les tutelles correspondantes (universités, CNRS, INSERM, INRIA, etc.).

Article 3. **Définitions**

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

- **Université** : l'université Bordeaux Montaigne.
- **Utilisateur** : toute personne ayant un lien de subordination juridique avec l'université Bordeaux Montaigne, qui est amenée à utiliser les services numériques de l'université Bordeaux Montaigne, quel que soit son statut.
  Le terme « Utilisateur » s'applique également à toute personne invitée, autorisée à utiliser les moyens informatiques de l'université dans le cadre de son activité professionnelle.
  Le terme « Utilisateur » s'applique également aux étudiants de l'université Bordeaux Montaigne.
  Le terme « Utilisateur » s'applique enfin aux prestataires ou personnes extérieures, dont l'accès aux services susvisés fait l'objet d'un lien contractuel spécifique avec l'université Bordeaux Montaigne (contrat de prestation, marché public, etc.). Ce contrat précise l'obligation de respect de la charte.
- **Administrateur** : toute personne (ou groupe de personnes) chargée de l'exploitation, de la maintenance et de la supervision d'un service numérique, ou d'une partie de ce dernier. Les Utilisateurs au sens de la présente charte ayant des fonctions d'Administrateurs doivent se conformer à la présente charte et à la charte d'Administrateurs, indépendante de la présente charte.
- **Services numériques** : ensemble de processus et de ressources mis à disposition par l'université, permettant d'acquérir, de générer, de traiter, de stocker, de détruire, de diffuser, de transmettre ou d'accéder à des informations électroniques.
- **Ressources numériques** : ensemble de moyens informatiques et de télécommunications, matériels ou logiciels, que l'université Bordeaux Montaigne met à disposition des Utilisateurs afin que ceux-ci puissent accomplir leurs tâches professionnelles. Ainsi, les micro-ordinateurs fixes ou portables, les moyens de communication (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 des ressources du système d'information de l'université Bordeaux Montaigne.

Article 4. **Principes directeurs**

Il appartient à chacun d'adopter un comportement professionnel et responsable lors de l'utilisation des services et des ressources numériques afin de ne pas perturber ou entraver leur bon fonctionnement, ni entrainer un détournement des activités à des fins non-professionnelles ou illégales.

4.1 Usage « professionnel » des services et des ressources numériques

L'ensemble des services et des ressources numériques est mis à disposition des Utilisateurs pour un usage professionnel, en tant que moyen utile à l'accomplissement des tâches ou missions qui leur sont confiées au titre de leur emploi.

4.2 Usage « privé » des services et des ressources numériques

L'utilisation à des fins privées des services et ressources numériques est tolérée dans la limite raisonnable liée aux nécessités de la vie courante et familiale.

Cet usage raisonnable à titre extra-professionnel doit être loyal, mesuré et ne peut en cas se faire au détriment des tâches ou missions professionnelles incombant à l'Utilisateur. Il ne doit en aucun cas nuire au bon fonctionnement de l'ensemble des ressources numériques de l'université ou altérer son image.

4.3 Confidentialité des informations et des données

La protection du patrimoine numérique de l'université et ses intérêts supposent le respect par chaque Utilisateur d'une obligation de confidentialité à l'égard des informations dont il a connaissance dans l'exercice de ses activités professionnelles. Les agents d'État sont notamment soumis à une obligation particulière de secret professionnel mais également de discrétion.

Dans ce cadre, l'Utilisateur se doit de respecter certaines règles :

- l'Utilisateur est soumis à une obligation de confidentialité. Il ne doit transmettre aucune information de l'université, notamment celles à caractère confidentiel, sans y être formellement autorisé ;
- l'Utilisateur ne doit pas tenter d'accéder ou prendre connaissance d'un message électronique qui serait adressé à un autre destinataire sans l'autorisation formelle de ce dernier ;
- en aucun cas, l'Utilisateur ne doit révéler à quiconque les moyens d'accès aux services et aux ressources numériques de l'université (ses mots de passe, code PIN ou tout autre secret d'authentification) qui sont strictement personnels et incessibles.

4.4 Dispositions législatives et réglementaires

Tout Utilisateur doit respecter les dispositions législatives et réglementaires relatives à l'utilisation des technologies de l'information et de la communication. Celles-ci prévoient en particulier les mesures interdisant :

- l'atteinte à la vie privée (i.e. opinions politiques, religieuses, philosophiques, aux origines ethniques, à la vie sexuelle ou à la santé des personnes) ;
- les actes de violence écrite ou verbale ou contraire aux règles éthiques ou aux bonnes mœurs, notamment :
  - la diffamation et l'injure,
  - le révisionnisme et l'apologie des crimes, notamment meurtre, viol, crime de guerre et crime contre l'humanité,
  - l'incitation aux crimes et délits (i.e. l'incitation au suicide, à la haine ou à la violence),
  - l'atteinte aux mineurs (i.e. exposition à des messages à caractère violent, pornographique ou pédopornographique),
  - l'incitation à la consommation de substances interdites ;

- la fraude informatique, incluant des actes tels que :
  - l'accès ou le maintien frauduleux dans un système de traitement automatisé de données,
  - la falsification, la modification, la suppression et l'introduction d'information avec l'intention de nuire ;
- la violation du secret professionnel, des affaires, des enquêtes et de l'instruction ;
- la violation de la propriété intellectuelle et du droit à l'image ;
- le non-respect de la réglementation relative à la protection des données à caractère personnel.

4.5 Conditions spécifiques d'usage des services et des ressources numériques par les organisations syndicales et les représentants du personnel

Il est rappelé que l'utilisation des ressources et services numériques par les organisations syndicales représentative et les représentants du personnel est régie par la décision du 22 février 2017 relative à l'utilisation par les organisations syndicales des technologies de l'information et de la communication.

4.6 Accès aux ressources et services numériques

Par principe, chaque Utilisateur n'a accès qu'aux services ou ressources numériques qui lui sont nécessaires dans le cadre de son activité professionnelle. Les droits d'accès à tout ou partie des services ou ressources numériques reposent sur une identification/authentification de chaque Utilisateur qui ne doit en aucun cas chercher à accéder par des moyens détournés ou fortuits à des informations et/ou ressources pour lesquelles il n'est pas habilité.

Les moyens d'authentification (i.e. mots de passe, code PIN ou tout autre moyen d'authentification) aux services ou ressources numériques sont strictement personnels et incessibles. Le respect de ces principes est de la responsabilité de l'Utilisateur.

4.7 Données personnelles de l'Utilisateur

La conservation de données, documents, fichiers et messages électroniques à titre privé est tolérée aux conditions strictes que l'usage soit raisonnable, que cela ne nuise pas au bon fonctionnement et la sécurité des services numériques, et que ces derniers ne contreviennent pas aux lois et à la réglementation en vigueur (i.e. données à caractère pédopornographique, pornographique, injurieux, diffamatoire, raciste, violent, faisant l'apologie du terrorisme ou d'actes illicites, etc.).

Ces données sont considérées comme privées dans la mesure où le marquage spécifique « PRIVE » ou « privé » est employé pour les identifier explicitement (dans le nom des fichiers, le nom du répertoire de stockage ou dans l'objet du message électronique).

Tout document, contenu ou message électronique qui ne comporterait pas ce marquage, sera alors considéré comme professionnel. L'université pourra y avoir accès même en l'absence de l'Utilisateur.

En application de ces principes, le répertoire « Mes documents » de chaque utilisateur est réputé professionnel. Cependant, l'espace de documents nommé « Privé » sur le bureau virtuel est considéré comme un espace privé.

L'Utilisateur ne doit, en aucun cas transformer et/ou qualifier des données, documents, fichiers ou messages de nature professionnelle en données, documents, fichiers ou messages privés.

4.8 Annuaire

L'Utilisateur est informé que ses coordonnées professionnelles figurent dans l'annuaire électronique de l'université. Cet annuaire est accessible :

- de l'intranet de l'université dans sa version complète ;

- sur le site Internet de l'université. L'Utilisateur a la possibilité de masquer son numéro de téléphone et son courrier électronique sur cet annuaire visible de tous en se mettant sur « liste rouge » via l'application « Mon compte ».

Il est aussi informé que sa photo peut figurer dans l'annuaire, uniquement s'il en donne explicitement l'accord via l'application « Mon compte ».

4.9 Protection du patrimoine numérique

L'université sauvegarde de manière automatique tout ou partie des données (répertoires, messages électroniques, etc.) présentes sur ses services et ressources numériques de manière à en garantir la disponibilité en cas d'incident. Les sauvegardes sont faites sans distinction des répertoires (privés ou non) de l'Utilisateur.

L'Utilisateur est toutefois responsable de la sauvegarde et de la récupération de ses données, fichiers, documents et messages électroniques marqués « PRIVE » ou « privé ».

4.10 Protection des informations contenues dans les équipements informatiques et supports amovibles

Le matériel informatique et de télécommunication que l'université fournit est placé sous la responsabilité de l'Utilisateur, en tous lieux et en toute circonstance.

A ce titre, l'Utilisateur doit utiliser les moyens de protection mis à sa disposition (câble antivol, armoire sécurisée, etc.) et appliquer les consignes de sécurité (verrouillage de l'ordinateur) afin de se prémunir contre le vol d'information. Lors de l'utilisation d'équipements nomades ou mobiles (notamment lors de voyages ou déplacements), les risques de compromission potentielle de l'information sont plus élevés. L'Utilisateur doit donc faire preuve d'une vigilance accrue pour en assurer la surveillance. En cas de perte ou de vol, il doit le signaler dans les plus brefs délais à son responsable hiérarchique et à son service informatique de proximité (qui informera le RSSI), qui lui indiquera la procédure à suivre.

Enfin, l'Utilisateur doit faire preuve d'une attention particulière lors de l'emploi des supports amovibles de stockage de masse (tels clés USB, disques durs externes, etc.) dont l'usage est fortement déconseillé. Pour les personnels de l'université, l'usage de supports amovibles de stockage de masse non fournis par l'université est interdit. Les supports de stockage fournis par l'université ne doivent pas être prêtés ni connectés à des ordinateurs autres que ceux fournis par l'université.

4.11 Protection du matériel

Chaque Utilisateur contribue à la protection des informations conservées sur les équipements mis à sa disposition. Dans cette perspective, il se doit notamment de respecter toutes les mesures élémentaires visant à ne pas introduire et diffuser de programmes malveillants, à ne pas entraver le bon fonctionnement des contrôles de sécurité ou y porter atteinte de manière volontaire. L'Utilisateur s'assure de :

- ne pas mettre en œuvre d'outils susceptibles de contourner ou d'affaiblir la sécurité des services numériques de l'université ;
- ne pas stocker, transférer ou transmettre des informations professionnelles, qu'elle qu'en soit leur nature, via des dispositifs non autorisés par l'université ;
- ne pas exploiter les éventuelles failles de sécurité, en faire la publicité ou les divulguer à des tiers ;
- ne pas altérer la configuration de ses équipements notamment en ce qui concerne le paramétrage des dispositifs de sécurité tels que l'antivirus, le pare-feu, le verrouillage de l'écran de veille, etc.

Seul le matériel mis à disposition par les services informatiques internes peut être connectés aux infrastructures informatiques et de télécommunication de l'université. En particulier, le matériel propriété

des prestataires intervenant pour le compte de l'université et ceux des visiteurs, ne peut être connecté qu'au réseau Wifi ou au réseau « invités.

Enfin, l'Utilisateur doit restituer tout matériel informatique et de télécommunication confié par les services Informatiques (poste de travail portable, téléphone mobile, etc.) lorsqu'il quitte ses fonctions.

4.12 Services Internet

L'utilisation d'Internet n'est autorisée que dans le cadre de l'activité professionnelle. Toutefois, un usage raisonnable des services de l'Internet est toléré dans le cadre des nécessités de la vie courante et familiale, à condition que son utilisation n'affecte pas les performances des services numériques de l'université ou ne perturbe pas le travail de l'Utilisateur.

L'université se réserve le droit de bloquer ou de limiter l'accès, au travers de dispositifs de filtrage ou de sécurité, à tout contenu présentant un risque légal, d'image ou d'atteinte à la sécurité de l'université ou des Utilisateurs tels qu'un site malveillant, pornographique, etc. ou incompatibles avec l'activité professionnelle.

Les contenus en ligne susceptibles d'entrainer une consommation importante des ressources Internet peuvent également être réglementés par l'université.

Par ailleurs, l'Utilisateur des services de l'Internet s'engage à ne pas utiliser les ressources de l'université pour tenir des propos (oraux ou écrits) qui seraient considérés comme illicites ou contraires à l'ordre public, à ne pas porter atteinte à l'intégrité d'un autre Utilisateur ou à sa sensibilité notamment par des messages, textes ou images provocants et à ne pas émettre d'opinion personnelle étrangère à son activité professionnelle ou susceptible de porter préjudice à l'université. Les Utilisateurs sont fortement encouragés à respecter les règles de politesse d'usage sur l'Internet.

4.13 Stockage en ligne

Le stockage et partage de fichiers sur des outils de stockage en ligne non explicitement autorisés par l'université est strictement interdit. En particulier, l'usage de Dropbox, Onedrive, Google drive, etc. est interdit pour stocker des fichiers professionnels.

Il est également strictement interdit d'utiliser les services externes d'échanges de fichiers volumineux, à l'exception de Filesender de Renater pour des données non sensibles.

4.14 Messagerie électronique

L'Utilisateur se voit attribuer une adresse électronique professionnelle lors de sa prise de fonction. Celle-ci est mise à sa disposition pour un usage strictement professionnel.

Cependant, un usage raisonnable et ponctuel de la messagerie électronique dans le cadre des nécessités de la vie courante et familiale est toléré, à condition que l'utilisation du courrier électronique n'affecte pas le trafic normal des messages professionnels. Tous les courriels, reçus ou sauvegardés depuis les ressources et services numériques de l'université sont présumés être professionnels, à défaut d'avoir été clairement identifiés comme « PRIVE » ou « privé » par l'Utilisateur.

L'Utilisateur ne doit pas transmettre d'information professionnelle sensible sur sa messagerie électronique privée ou celle d'un tiers, ou au travers de services numériques de l'Internet, sauf autorisation express par un accord dans le cadre d'une situation exceptionnelle (par exemple en cas de gestion de crise déclarée ainsi par les services compétents).

La redirection des messages électroniques vers une boite électronique privée est fortement déconseillée car cela peut constituer une fuite irrémédiable d'informations confidentielles de l'université. De plus les messageries personnelles sont généralement moins bien sécurisées que les messageries professionnelles. Un

cybercriminel pourrait donc accéder plus facilement aux données confidentielles de l'université qui seraient conservées dans une messagerie personnelle.

Si l'Utilisateur reçoit par erreur un message dont il n'aurait pas dû être destinataire, toute utilisation, copie ou diffusion, même partielle de ce message est interdite. Il a l'obligation de le détruire et d'en informer immédiatement son expéditeur. Cette règle ne s'applique pas si le message tombe dans le champ de l'article 40 alinéa 2 du code de procédure pénale :

> *Toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs.*

Par ailleurs, l'Utilisateur est informé de la mise en place de quotas individuels au niveau de chaque boîte aux lettres électronique et d'un filtrage des courriels reçus et envoyés (quotas d'envoi ou de réception, fichiers autorisés, etc.)

En cas d'absence planifiée, l'Utilisateur active, dans la mesure du possible, le dispositif de notification d'absence.

4.15 Alias de messagerie électronique

Un alias d'adresse électronique, fonctionnel ou organisationnel, peut être mise en place pour un utilisateur ou un groupe d'utilisateurs pour les besoins de l'université. Il ne s'agit pas d'une adresse physique mais d'un lien vers l'adresse nominative de l'Utilisateur.

La gestion d'adresses électroniques correspondant à des listes de diffusion institutionnelles, désignant une catégorie ou un groupe d'Utilisateurs, relève de la responsabilité exclusive de l'université : ces adresses ne peuvent être utilisées sans autorisation explicite.

4.16 Messagerie instantanée

L'utilisation des messageries instantanées publiques telles que WhatsApp, Telegram, Signal ou Facebook Messenger à titre professionnel est interdit, du fait des risques de captation ou de fuite d'information.

L'Utilisateur doit privilégier les services de messagerie instantanée de l'université ou ceux proposées par les services de l'Etat.

4.17 Médias sociaux

L'Utilisateur est responsable de l'information qu'il communique sur les médias sociaux tels que les forums, les blogs, réseaux sociaux, etc. Il respectera son devoir de réserve lorsqu'il s'exprimera sur ces médias. Il est donc recommandé à l'Utilisateur de communiquer et de publier des contenus, avec une extrême prudence.

Il est rappelé que des sanctions peuvent être appliquées en cas de divulgation d'informations sensibles ou d'atteinte à l'image de l'université.

Article 5. **Règles d'utilisation spécifiques**

5.1 Accès distant et mobilité

En accédant aux services numériques de l'université à distance, l'Utilisateur emprunte des infrastructures de télécommunication publiques, non maitrisées par l'université et par défaut non réputées sûres. Cet accès ne peut donc se faire que dans un cadre précis :

- l'Utilisateur doit utiliser les mécanismes d'accès à distance fournis par l'université pour se connecter à distance aux ressources de l'université ;
- L'université se réserve le droit de conserver et d'analyser les traces relatives aux accès distants des Utilisateurs et actions effectuées sur les services et ressources numériques.

L'attention de l'utilisateur est appelée sur l'utilisation des ressources et services numériques en mobilité qui présente des risques plus élevés et des conséquences plus importantes, notamment lors des déplacements à l'étranger compte-tenu des formalités douanières de certains pays étrangers (Etats-Unis et Chine en particulier).

Pour éviter, toute captation d'information par les autorités douanières, l'Utilisateur veille à emporter avec lui uniquement le matériel professionnel et la quantité d'informations utiles à sa mission. En cas d'interception par les autorités douanières, l'Utilisateur doit signaler l'incident dans les plus brefs délais à son responsable hiérarchique et à son service informatique de proximité, qui lui indiquera la procédure à suivre.

5.2 Objets connectés

Les objets connectés personnels (montres, écouteurs sans fil, smartphones, tablettes, etc.) utilisés à titre privé ne doivent pas être branchés aux équipements professionnels. L'Utilisateur doit être conscient que l'introduction dans l'enceinte de l'université d'objets connectés peut engendrer des risques supplémentaires tels que la captation d'informations, la géolocalisation des biens et des personnes, ou la propagation de programmes malveillants.

L'utilisateur est informé que l'utilisation de ce type de matériel peut être réglementée de manière plus stricte (limitation ou interdiction d'usage) en fonction de son emploi, de sa structure d'accueil ou d'appartenance.

Article 6. **Conditions d'utilisation spécifiques**

6.1 Modalités relatives au télétravail

Le télétravail désigne toute forme d'organisation du travail dans laquelle une tâche qui aurait également pu être exécutée dans les locaux de l'université est réalisée par un Utilisateur en dehors de ces locaux de façon régulière et volontaire.

L'accès au télétravail relève du responsable hiérarchique de l'Utilisateur, ou de circonstances exceptionnelles. Les dispositions de la présente charte s'appliquent au télétravail et aux usages en mobilité des services numériques de l'université. Pour des raisons de sécurité, l'accès aux ressources ou services numériques en télétravail peut être réglementé (limitation d'accès voire interdiction) par le responsable de traitement ou le service du haut fonctionnaire de défense et de sécurité.

6.2 Droit à la déconnexion

Pendant les périodes de repos, congés et suspension du travail, il convient de s'assurer d'un usage raisonnable et conforme des services et des ressources numériques. Par exemple, l'usage de la messagerie électronique ou du téléphone professionnel, en dehors des horaires de travail, doit se faire en respectant la vie privée du destinataire et de l'émetteur et le droit à la déconnexion du destinataire et de l'émetteur, sauf pour faire face à une situation d'urgence.

6.3 Nécessité impérieuse de service

En cas d'absence et pour des raisons exceptionnelles, l'accès à une copie des ressources informatiques de l'Utilisateur (messagerie électronique, base collaborative, répertoire réseau, poste de travail, ou tout service

numérique ou matériel informatique et de communication), peut être autorisé en cas de nécessité par son supérieur hiérarchique. Ce dernier doit pour cela en faire la demande expresse au directeur de la DSIN et en informer en parallèle le responsable des ressources humaines. La DSIN sera chargée alors de faire le nécessaire afin de ne pas communiquer de données privées.

Dans tous les cas, l'intéressé est averti des demandes d'autorisation d'accès à ses ressources.

Article 7. Protection des propriétés intellectuelles, des informations et des données

7.1 Données à caractère personnel

L'Utilisateur s'engage à préserver les données à caractère personnel, traitées par les services numériques de l'université, conformément à la loi nº 78-17 du 6 janvier 1978 dite « informatique et libertés » modifiée par la loi nº 2004-801 du 6 août 2004 et du règlement général de protection des données du 27 avril 2016. La perte, la destruction ou la divulgation frauduleuses, accidentelles ou non autorisées de données personnelles pourraient avoir des conséquences graves pour l'université.

Les données à caractère personnel sont des informations qui permettent - sous quelque forme que ce soit - directement ou indirectement, l'identification des personnes physiques auxquelles elles s'appliquent.

L'Utilisateur se doit de :

- respecter les finalités définies, explicites et légitimes d'un traitement comportant des données personnelles (l'utilisation de données à caractère personnel pour une finalité non autorisée constitue un « délit de détournement des données ») ;
- protéger les données personnelles afin qu'elles ne soient pas utilisées par des personnes non autorisées ou habilitées, ni divulguées, supprimées ou détruites, perdues, volées, même de manière accidentelle (cela suppose le contrôle rigoureux de la diffusion de données à caractère personnel à destinataire de tiers extérieurs à l'université) ;
- respecter et donc ne pas contourner, ni désactiver, les mesures techniques, organisationnelles et juridiques, prises par l'université pour assurer la protection des données à caractère personnel.

A ce titre, toutes les créations de fichiers comprenant ce type d'informations et demandes de traitement afférent, y compris lorsqu'elles résultent de croisement ou d'interconnexion de fichiers préexistants, sont soumises aux formalités préalables prévues par la loi « Informatique et Libertés ».

En conséquence, tout utilisateur souhaitant procéder à une telle création devra en informer préalablement le délégué à la protection des données (dpd@u-bordeaux-montaigne.fr) de l'université qui prendra les mesures nécessaires au respect des dispositions légales.

Par ailleurs, conformément aux dispositions de la loi et du règlement, chaque utilisateur dispose d'un droit d'accès et de rectification relatif à l'ensemble des données le concernant, y compris les données portant sur l'utilisation du système d'information.

Ce droit s'exerce auprès du délégué à la protection des données (DPO) de l'établissement

7.2 Propriété intellectuelle et droit à l'image

L'Utilisateur s'interdit de produire, de collecter/télécharger/utiliser ou de transmettre des données, des fichiers, des logiciels, des applications, des messages, des œuvres ou des contenus protégés, quel qu'en soit le support, la nature ou la forme (par exemple photographie, dessins, écrit, enregistrement musical ou vidéo, image, logo, logiciel, etc.), qui ne soient pas dans le respect du droit de propriété intellectuelle, du droit à l'image ou du droit à la vie privée.

L'attention de l'utilisateur est appelée sur les poursuites pénales et/ou civiles dont lui-même et/ou l'université pourraient faire l'objet du fait de la rediffusion, par quelque moyen que ce soit, de messages répréhensibles captés sur le réseau internet ou de l'utilisation, de la diffusion, voire du simple enregistrement informatique, d'œuvres ou de données en contravention avec les législations existantes ou sans l'autorisation des titulaires des droits.

Article 8. **Sécurité et cyber surveillance**

8.1 Signalement

L'Utilisateur se doit de signaler dans les plus brefs délais tout constat, tentative ou soupçon de violation de ses droits d'accès au RSSI ou correspondant SSI de proximité. La participation des Utilisateurs à la détection d'anomalies et d'un incident de sécurité sur les services numériques est déterminante dans la rapidité de mise en œuvre des mesures de protection.

En cas de perte ou de vol de moyens d'authentification, l'Utilisateur doit en informer sans délai son supérieur hiérarchique, le RSSI ou correspondant SSI de proximité et mettre en œuvre les démarches nécessaires, notamment pour limiter l'accès aux données professionnelles et aux services numériques de l'université.

8.2 Surveillance des ressources et services numériques

Pour garantir la sécurité des services et ressources numériques et la protection des informations nécessaires au bon fonctionnement de l'université, le RSSI peut, sans préavis, limiter ou bloquer l'accès à certains services numériques, sites Web, ressources ou à certaines parties de l'Intranet, à tous ou bien certains Utilisateurs, pour une durée indéterminée.

Il est susceptible de mettre en œuvre des mécanismes de filtrage et d'analyser du trafic réseau, même chiffré. Des moyens de déchiffrement pourront être appliqués à l'ensemble des flux de connexion des Utilisateurs, à l'exception de ceux qui seront inclus au sein d'une « liste blanche de sites » qui ne feront pas l'objet d'un déchiffrement de flux et de ceux dont le déchiffrement est interdit par la loi.

Il est interdit de les contourner ou de tenter de les contourner, sous peine de sanction.

8.3 Traçabilité

Pour garantir une traçabilité et être en mesure de fournir des preuves, notamment en cas d'enquête, l'université conserve, en fonction de la finalité et des durées fixées par les textes applicables, les journaux d'accès et d'utilisation générés dans les services ou ressources numériques qu'il met en œuvre. Cette conservation est réalisée dans le respect des dispositions réglementaires relatives à la protection des données personnelles.

8.4 Suivi des acquis en matière de sécurité numérique

L'université informe les Utilisateurs par des campagnes de sensibilisation à la sécurité des services numériques et de vérification générale de leur bonne utilisation qu'elle organise. Les résultats de ces campagnes seront anonymisés et ne pourront pas conduire à une sanction quelconque.

Article 9. **Contrôle, maintenance et gestion des services et des ressources numériques**

9.1 Opérations de maintenance et de contrôle

Une opération de maintenance s'inscrit dans le cadre d'une opération programmée de maintien en bon état de fonctionnement des moyens considérés. La maintenance peut être opérée par des personnels internes ou des prestataires extérieurs, aussi bien sur le lieu de travail, à distance (télémaintenance) ou encore au domicile de l'Utilisateur (cas particulier du télétravail).

Les ressources numériques de l'université font l'objet de contrôles ayant comme unique finalité d'assurer la sécurité et la continuité des ressources et des données de l'université. En cas d'événement ou d'anomalie liés à la sécurité ou à la continuité de ses systèmes, l'université s'autorise à prendre toutes les mesures nécessaires pour en identifier les causes.

L'université se réserve le droit de consulter de manière exceptionnelle le contenu des documents, fichiers ou messages, identifiés « PRIVE » ou « privé » de l'Utilisateur en cas de risque de mise en péril de son activité, par exemple la présence de code malveillant, en cas d'urgence ou dans le cas d'une enquête judiciaire en cours.

La collecte de données personnelles sera limitée aux informations nécessaires à la sécurité des services et des ressources numériques. Ces données sont conservées pour une durée maximale de 6 mois après collecte.

Les éléments découverts à l'occasion d'une opération de contrôle ou de maintenance sont susceptibles de constituer des moyens de preuves licites contre les agissements d'un Utilisateur.

L'Utilisateur s'engage à ne pas entraver toute opération de contrôle ou de maintenance effectuée par les services informatiques de l'université.

9.2 Moyens de télécommunication.

La mise à disposition au bénéfice de l'Utilisateur d'une ligne téléphonique, fixe et/ou mobile, conduit l'université à disposer des données relatives à l'utilisation de ces moyens de communication, que ces données soient issues des systèmes de téléphonie internes ou de leur transmission par l'opérateur auprès duquel l'université est client.

Les smartphones, pouvant être mis à disposition de l'Utilisateurs par l'université, entrent dans ce cadre. Ces matériels qui permettent, de plus, le stockage de données, l'accès à Internet et à la messagerie électronique professionnelle, sont également soumis aux dispositions du présent document.

Des contrôles sont effectués pour détecter les lignes inutilisées ou les consommations anormales et déclencher éventuellement des analyses détaillées. Par ailleurs, des analyses globales portant sur les volumes des consommations et des coûts sont effectuées en vue d'optimisation économique.

En cas d'abus ou de dépassement non justifié de forfait, l'université se réserve la possibilité d'enquêter.

Article 10. **Responsabilités et sanctions**

Le non-respect des règles d'utilisation et des mesures de sécurité figurant dans la présente charte est susceptible de justifier la suspension immédiate de l'utilisation de tout ou partie des services et ressources numériques, et/ou l'engagement de poursuites disciplinaires adaptées à la gravité des agissements constatés, sans préjudice d'éventuelles actions pénales ou civiles à l'encontre de l'Utilisateur.

FIN DE LA CHARTE