Bordeaux INP AQUITAINE

E N S C
ENSCBP
ENSEGID
ENSEIRB
MATMECA
ENSPIMA
ENSTBB
ENSGTI*
ENSI Poitiers*
ISA BTP*
LA PRÉPA DES INP

# ANNEXE 4

## Charte d'utilisation des moyens et outils d'information et de

## Préambule

Bordeaux INP met en œuvre un système d'information et de communication nécessaire à l'exercice de ses missions. Il met ainsi à disposition de ses collaborateurs et usagers des outils informatiques et des moyens de communication.

La présente charte définit les conditions d'accès et les règles d'utilisation des outils informatiques et des moyens de communication de Bordeaux INP. Elle a également pour objet de sensibiliser les utilisateurs aux risques liés à l'utilisation de ces ressources en termes d'intégrité et de confidentialité des informations traitées ainsi que de sécurité informatique. Ces risques imposent le respect de règles de sécurité et de bonne conduite. L'imprudence, la négligence ou la malveillance d'un utilisateur peuvent en effet avoir des conséquences graves de nature à engager sa responsabilité civile et/ou pénale ainsi que celle de l'établissement.

L'article 41 du règlement intérieur de Bordeaux INP subordonne pour tout utilisateur, l'utilisation des ressources informatiques de Bordeaux INP à la prise de connaissance et à l'acceptation de la présente « Charte d'utilisation des moyens et outils d'information et de communication de Bordeaux INP » qui fait partie intégrante dudit règlement intérieur.

La procédure d'ouverture des comptes informatique de Bordeaux INP comprend une étape incontournable d'acceptation de la présente charte.

À chaque modification, la charte est diffusée à l'ensemble des utilisateurs par mail. Elle est disponible sur l'espace de travail de Bordeaux INP. Des actions de communication internes sont organisées afin d'informer les utilisateurs des pratiques recommandées.

## Définitions

- → **Délégué à la protection des données (DPD ou DPO)** : correspondant, désigné par le directeur général de Bordeaux INP, en charge de mettre en œuvre la conformité du règlement européen sur la protection des données au sein de Bordeaux INP.
- → **Données à caractère personnel** : toute information se rapportant à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.
- → **Équipements nomades** : tous les moyens techniques mobiles (ordinateur portable, imprimante portable, tablette, téléphone mobile ou smartphone, objet connecté, CD ROM, clé USB, disque dur amovible…)
- → **Information d'authentification** : identifiant, mot de passe, code PIN, clés privées, etc.
- → **Information professionnelle** : information utilisée en contexte de travail. Elle peut être nuancée : publique, interne, confidentielle, secrète.
- → **Outils informatiques et de communication** : tous les équipements informatiques, de télécommunications et de reprographie de Bordeaux INP.

→ **Parrain :** personnel de l'établissement qui est responsable de la création et de la suppression du compte informatique associé d'un vacataire ou d'un hébergé. Il effectue la demande de création du compte en précisant sa durée. Il est destinataire de toute notification relative à la durée de vie du compte et peut demander éventuellement sa prolongation, à échéance.
→ **Responsable de la sécurité des services d'information (RSSI)** : personne, désignée par le directeur général de Bordeaux INP, qui définit la politique de sécurité du service d'information et qui veille à son application.
→ **Sécurité physique** : concerne tous les aspects liés à l'environnement dans lequel les systèmes se trouvent.
→ **Sécurité logique** : réalisation de mécanismes techniques de sécurité par logiciel.
→ **SIM** : Service Informatique Mutualisé de Bordeaux INP.
→ **Site malveillant** : tout site conçu pour faire accomplir à un utilisateur légitime des actions indésirables ou néfastes pour la sécurité du système d'information.
→ **Structure** : entité administrative ou d'enseignement ou de recherche rattachée à Bordeaux INP (services généraux, écoles, La Prépa des INP, laboratoires, etc.).
→ **Systèmes d'information** : ensemble de ressources matérielles, logicielles, applications, base de données et réseaux de télécommunications mis à disposition par Bordeaux INP.
→ **Tiers** : une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel.
→ **Traitement des données** : opérations informatisées portant sur des données telle que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement et la destruction.
→ **Utilisateur Bordeaux INP** : personnels (agents titulaires ou contractuels, vacataires) et étudiants de Bordeaux INP autorisés à accéder et à utiliser les outils informatiques et moyens de communication de Bordeaux INP.
→ **Utilisateur hébergé** : personnels des laboratoires hébergés au sein de Bordeaux INP ou étudiants d'un autre établissement du site accueillis pour un enseignement autorisés à accéder et à utiliser les outils informatiques et moyens de communication de Bordeaux INP

## Article 1 – Champ d'application

La présente charte s'applique à tout utilisateur du système d'information et de communication de Bordeaux INP, qu'il soit personnel, étudiant de l'établissement ou hébergé en son sein.

## Article 2 – Droits d'accès au système d'information

L'accès au système d'information (ressources informatiques, service Internet, réseau…), est accordé selon les conditions suivantes :

| | Utilisateurs Bordeaux INP | | | Utilisateurs hébergés |
|---|---|---|---|---|
| À qui est accordé l'accès ? | Personnels de Bordeaux INP | | Etudiants de Bordeaux INP | |
| | Enseignants/ chercheurs, BIATSS, titulaires et contractuels | Vacataires | | |
| L'accès est accordé à compter de quand ? | Dès la prise de fonction | À la date de la prise en compte de la demande d'un parrain | Dès l'inscription dans une des écoles de Bordeaux INP | À la date de la prise en compte de la demande expresse motivée d'un parrain |
| L'accès est accordé pour quelle durée ? | Pendant la durée des fonctions | Jusqu'au 31 août de l'année universitaire en cours | Pendant la durée des études dans l'établissement | Défini lors de la demande, ne peut excéder un an. Renouvelable par un parrain |
| L'accès est-il maintenu ensuite ? | 1 mois | Le compte peut être prolongé par période d'un an maximum, renouvelable autant que nécessaire, par le parrain sinon 1 mois | Jusqu'au 31 janvier de l'année suivant l'obtention du diplôme | Le compte peut être prolongé par période d'un an maximum, renouvelable autant que nécessaire, par le parrain sinon 1 mois |
| À quel moment les données sont-elles supprimées ? | 1 mois après la fermeture du compte<br>2 mois en cas de départ imprévu | 1 mois après la fermeture du compte | 1 an après la fermeture du compte | 1 mois après la fermeture du compte |

Le Directeur Général de Bordeaux INP peut décider à titre conservatoire de limiter, suspendre ou retirer l'accès au système d'information si le comportement de l'utilisateur n'est pas en adéquation avec la présente charte ou présente un risque pour l'intégrité du système d'information.

Ce droit d'accès est personnel et ne peut être cédé même temporairement à un tiers, il est matérialisé par la création d'identifiants nominatifs et confidentiels (couple login / mot de passe).

Un utilisateur ne peut en aucun cas permettre à une autre personne, d'accéder au système d'information de l'établissement au moyen de ses identifiants. Dans ce cas, l'utilisateur engage sa responsabilité et reste pleinement responsable des actions effectuées avec ses identifiants.

## Article 3 – Conditions d'utilisation du système d'information

Chaque utilisateur accède aux outils informatiques nécessaires à l'exercice de son activité professionnelle ou d'études dans les conditions définies par Bordeaux INP.
L'utilisateur est responsable, en tout lieu, de l'usage qu'il fait du système d'information auquel il a accès.
Il a une obligation de réserve et de confidentialité à l'égard des informations et documents auxquels il accède.
Cette obligation implique le respect des règles d'éthique et de déontologie.

### Article 3.1 – Confidentialité

L'information collectée et contenue dans les fichiers et les bases de données exploitées par l'établissement a un caractère confidentiel.

Tout utilisateur autorisé à accéder aux données du système d'information de Bordeaux INP s'engage à maintenir confidentielle l'information à laquelle il a accès dans le cadre de ses fonctions.

Il doit être vigilant vis-à-vis des données auxquelles il accède et être attentif au respect des règles de la politique de sécurité des systèmes d'information.

L'utilisateur est responsable des fichiers et répertoires qu'il constitue.

Il est interdit de prendre connaissance d'informations détenues par d'autres utilisateurs sans leur accord, quand bien même ceux-ci ne les auraient pas correctement protégées.

L'utilisateur ne doit pas tenter d'intercepter des communications entre tiers.

### Article 3.2 – Utilisation dans le cadre professionnel ou des études / privé

Le système d'information est composé d'outils de travail permettant pour les personnels la réalisation d'activités de recherche, d'enseignement et d'administration et pour les étudiants d'études et de vie étudiante. Toute information traitée dans ce cadre est réputée relever du cadre professionnel ou des études, à l'exclusion des données explicitement désignées par l'utilisateur comme relevant de sa vie privée. Il appartient à l'utilisateur de procéder au stockage et à la sauvegarde de ces données dans un dossier intitulé « Privé ». Le cas échéant, la sauvegarde régulière des données privées incombe à l'utilisateur. En aucun cas, la responsabilité de l'établissement ne pourra être engagée quant à la conservation des données privées.

L'utilisation du système d'information à titre privé doit être non lucrative et raisonnable, tant dans sa fréquence que dans sa durée. En toute hypothèse, le surcoût qui en résulte doit demeurer négligeable au regard du coût global d'exploitation et ne pas nuire au bon fonctionnement de l'établissement.

L'utilisation des systèmes d'information à titre privé doit respecter la réglementation en vigueur. Par exemple, le téléchargement illégal, la détention, la diffusion et exportation d'images à caractère pédophile, ou la diffusion de contenus à caractère raciste ou antisémite est interdite.

L'utilisation d'équipements personnels (ordinateurs, smartphones, tablettes, etc. achetés sur des fonds personnels), pour accéder localement ou à distance aux ressources de Bordeaux INP, doit être conforme aux préconisations de la politique de sécurité des systèmes d'information de Bordeaux INP.

En aucun cas, des données professionnelles (qui sont la propriété de Bordeaux INP) ne doivent être enregistrées ou stockées sur des ressources informatiques personnelles.

### Article 3.3 – Continuité de service : gestion des absences et des départs des personnels

Il appartient à l'utilisateur (personnel) de suivre les recommandations de son responsable hiérarchique (usage des espaces partagés et alias de messagerie) concernant l'accessibilité des données liées à son activité professionnelle. Aux seules fins d'assurer la continuité de service, l'utilisateur veillera, notamment à ce que celles-ci soient accessibles à son supérieur hiérarchique, en cas de départ ou d'absence.

Dans le cas d'un départ ou d'une absence, si les données numériques, à caractère professionnel, n'étaient pas accessibles, le responsable peut demander au SIM d'accéder à tous les documents et informations professionnelles (hors dossier « Privé »). L'accès à ces données se fait alors par un membre du SIM en présence du responsable et du DPD. En cas d'absence du DPD, il peut être remplacé par le RSSI ou le Directeur des Systèmes d'Information.
Le supérieur hiérarchique peut également demander au SIM de mettre un message d'absence sur la messagerie électronique de l'agent.

Lors de son départ, l'utilisateur doit restituer au SIM les matériels (ordinateurs portables, téléphones, disques durs externes, clé USB, etc.) mis à sa disposition par Bordeaux INP.

## Article 4 – Outils de communication

### Article 4.1 – Messagerie électronique

L'utilisation de la messagerie constitue un élément essentiel d'optimisation du travail, de mutualisation et d'échange de l'information au sein de Bordeaux INP.

#### Adresses électroniques

Bordeaux INP met à disposition de l'utilisateur une adresse électronique professionnelle/étudiante nominative lui permettant d'émettre et de recevoir des messages. L'utilisation de cette adresse électronique relève de la responsabilité de son détenteur. Son utilisation est interdite sur des sites sans rapport avec son activité professionnelle. L'aspect nominatif de l'adresse électronique constitue le simple

prolongement de l'adresse administrative : il ne retire en rien le caractère professionnel de la messagerie.

**L'adresse électronique mise à disposition sera celle utilisée par l'administration pour transmettre à l'utilisateur toute information utile. Sa consultation régulière est donc une obligation.**

Une adresse électronique fonctionnelle ou organisationnelle, peut être mise en place pour un utilisateur ou un groupe d'utilisateurs pour les besoins de Bordeaux INP.

La gestion des adresses électroniques correspondant à des listes de diffusions institutionnelles, désignant une catégorie ou un groupe d'utilisateurs, relève de la responsabilité de Bordeaux INP.

L'utilisateur est inscrit automatiquement à des listes de diffusion électroniques institutionnelles, thématiques ou syndicales. À l'exclusion des listes institutionnelles, il peut demander à en être désinscrit.

### Contenu des messages électroniques

Tout message est réputé professionnel. Les messages à caractère personnel sont tolérés, ils doivent être signalés par la mention « Privé » dans leur objet et être classés dès l'envoi ou la réception dans un dossier nommé « Privé ».

Les utilisateurs ne doivent pas faire circuler par mail des informations contenant des listes de données à caractère personnel ou des données concernées par le dispositif de protection du potentiel scientifique et technique (PPST).

Les messages envoyés peuvent engager la responsabilité civile ou pénale de Bordeaux INP ou de l'utilisateur.

Sont interdits les messages comportant des contenus à caractère illicite quelle qu'en soit la nature : il s'agit notamment des contenus contraires aux dispositions de la loi sur la liberté d'expression ou portant atteinte à la vie privée d'autrui (exemple : diffamation, injure…).

Les messages électroniques échangés avec des tiers peuvent, au plan juridique, former un contrat, sous réserve du respect des conditions fixées par les articles 1369-1 à 1369-11 du code civil. L'utilisateur doit, en conséquence, être vigilant sur la nature des messages électroniques qu'il échange au même titre que pour les courriers traditionnels. Le courrier est un document administratif reconnu en tant que preuve en cas de contentieux.

### Émission et réception des messages

L'utilisateur doit s'assurer de l'identité et de l'exactitude des adresses des destinataires des messages.
Il doit veiller à ce que la diffusion des messages soit limitée aux seuls destinataires concernés afin de préserver le bon fonctionnement du service de messagerie. De même, la taille, le nombre et/ou le type de pièces jointes, peuvent être limités pour éviter l'engorgement ou la dégradation du système de messagerie.

Les messages électroniques envoyés font l'objet d'un contrôle automatique antiviral. Le risque de retard, de non remise ou de suppression automatique des messages électroniques doit être pris en considération lors d'envoi de correspondances

importantes.

Les messages électroniques reçus font l'objet d'un contrôle automatique antiviral et anti-spam. L'utilisateur doit faire preuve de vigilance vis-à-vis des informations reçues (désinformation, virus informatique, hameçonnage, tentative d'escroquerie…).

La capacité de stockage des messages électroniques est limitée. Le SIM peut donc demander aux utilisateurs de supprimer des messages. Si l'utilisateur souhaite conserver ses messages, il lui appartient de les archiver.

### Article 4.2 – Internet

Il est rappelé qu'internet est soumis au respect de l'ensemble des règles de droit en vigueur.

L'établissement est signataire de la charte RENATER (Réseau National de télécommunications pour la Technologie, l'Enseignement et la Recherche). Dans ce cadre, il se doit de faire respecter les règles déontologiques qui y sont décrites.

La consultation de site à contenus de caractère pornographique ou illicite est interdite.

L'outil internet mis à disposition permet de consulter tous types de sites présentant un lien direct et nécessaire avec l'activité professionnelle ou de formation de l'utilisateur. Toutefois, une utilisation ponctuelle et raisonnable, pour un motif personnel, des sites internet dont le contenu n'est pas contraire à la loi, à l'ordre public, et ne mettant pas en cause l'intérêt et la réputation de l'établissement, est admise. En cas de suspicion d'atteinte à la sécurité du système d'information et des données de Bordeaux INP, tous les flux chiffrés (ex. : https, smtps, imaps…) peuvent être décryptés.

Les utilisateurs se doivent d'adopter un comportement loyal vis-à-vis de Bordeaux INP lors de l'utilisation des réseaux sociaux, des blogs, qu'ils soient professionnels (Linkedin, Viadéo, etc.) ou non professionnels (Facebook, Twitter, etc.).

Les données à caractère personnel ou les données concernées par le dispositif de protection du potentiel scientifique et technique (PPST), ne peuvent être déposées que sur des « clouds » dont les règles de sécurité sont maîtrisées et validées par Bordeaux INP.

### Article 4.3 – Téléchargements

Le téléchargement de logiciels ou d'œuvres protégées doit s'effectuer dans le respect des droits de la propriété intellectuelle tels que définis à l'article 7 et doit être fait dans le cadre d'usages professionnels.

Bordeaux INP se réserve le droit de limiter le téléchargement de certains fichiers pouvant se révéler volumineux ou présenter un risque pour la sécurité des systèmes d'information (virus susceptible d'altérer le bon fonctionnement du système d'information de Bordeaux INP, codes malveillants, programmes espions…).

### Article 4.4 – Publication sur les sites internet et intranet de Bordeaux INP

Le directeur général de Bordeaux INP, en tant que représentant légal, est le directeur de publication de l'établissement pour les sites internet mis en œuvre par l'établissement. Toute publication de pages d'information sur les sites internet et intranet de Bordeaux INP doit être conforme à la politique internet de l'établissement et validée par un

responsable de publication désigné.

Préalablement à un projet de diffusion sur un site internet, ou extranet d'informations relatives à des personnes, le service prendra attache auprès du délégué à la protection des données (DPD). Aucune publication de pages d'information à caractère privé n'est autorisée sur les ressources du système d'information de Bordeaux INP, sauf cas particulier autorisé par le Directeur Général.

Chaque site rattaché au nom de domaine de l'établissement doit comporter les mentions légales obligatoires et pointer également sur la rubrique dédiée « mentions légales » du site de Bordeaux INP.

Les informations publiées sur les sites du domaine de Bordeaux INP doivent être fiables et régulièrement mises à jour.

### Article 4.5 – Moyens de communication mobiles

L'octroi des moyens de communication mobiles (abonnements, téléphones mobiles et clés 4G) est limité aux seuls agents de l'établissement en ayant un besoin avéré pour la fonction qu'il ou qu'elle occupe. Les fonctions ouvrant droit à l'obtention d'un tel moyen sont :

- Directeur-rice général-e [(1)];
- Vice-Président-e en charge de la formation [(2)] ;
- Vice-Président-e en charge de la recherche et du transfert [(2)] ;
- Vice-Président-e en charge des relations internationales [(2)] ;
- Vice-Président-e en charge du numérique [(2)] ;
- Directeur-rice général-e des services [(2)] ;
- Chargé-e de mission [(2)] ;
- Directeur-rice d'école et de La Prépa des INP de Bordeaux [(2)] ;
- Directeur-rice de laboratoire ;
- Directeur-rice adjoint-e d'école ;
- Directeur-rice adjoint-e de laboratoire ;
- Directeur-rice des études d'école ;
- Responsable de filière ;
- Responsable administratif d'école ou de laboratoire ;
- Directeur-rice d'un service général ;
- Conseiller-ère de prévention ;
- Responsable du service logistique ;
- SSIAP ;
- Responsable technique de site ;
- Chargé de la maintenance des bâtiments ;
- Itinérant technique.

L'agent doit établir sa demande de moyen de communication mobiles auprès de l'ordonnateur principal ou secondaire lié à sa composante de rattachement. Pour le-la directeur-rice général-e, la demande doit être faite auprès du-de la directeur-rice général-e des services. Pour les fonctions annotées par un [(2)], la demande doit être faite auprès du-de la directeur-rice général-e.

L'ordonnateur appréciera la pertinence d'attribuer un tel moyen selon les critères suivants, cumulatifs ou non :

- Nécessité de continuité de service et de communication avec la hiérarchie et avec le public ;
- Fréquence des déplacements ou des réunions conduisant à une mobilité avérée ;
- Nombre de lieux de travail ;

- Nécessité d'astreinte hors plage horaire standard ;
- Responsabilité en termes de sécurité des biens et des personnes ou liée à des risques spécifiques.

Les moyens de communication mobiles sont ceux proposés dans le catalogue de l'opérateur retenu pour le marché public (https://www.bordeaux-inp.fr/extranet/fr/direction-financiere/marches-en-cours).
Le marché propose des abonnements, des téléphones mobiles (standards ou smartphones) et des clés 4G. La liste des modèles varie selon l'évolution technique des références proposées et les conditions du marché. Le demandeur et l'ordonnateur peuvent indiquer une préférence d'appareil sur la demande d'attribution de moyens de communication mobiles. Bordeaux INP se réserve le droit d'attribuer à l'agent n'importe quel appareil disponible au moment de l'achat qui permette de répondre au besoin.

Un terminal personnel peut être utilisé avec un abonnement professionnel. Dans ce cas de figure, l'établissement n'intervient pas sur l'appareil personnel et ne prend pas en charge les réparations éventuelles.

Le matériel confié à l'agent par Bordeaux INP relève du cadre strictement professionnel. L'utilisation à des fins étrangères au service peuvent relever d'une faute que Bordeaux INP se réserve le droit de poursuivre. Toutefois, une tolérance est admise quand l'utilisation personnelle qui en est faite reste raisonnable (appels au domicile de courte durée, brève consultation de serveurs pratiques sur internet, etc.) sous réserve que cet usage n'entrave pas l'activité professionnelle.

L'agent prend le plus grand soin du matériel qui est lui est confié. En cas de panne, vol ou casse, il en informe dans les plus brefs délais le service achats de Bordeaux INP (marches@bordeaux-inp.fr).

L'agent demandeur et l'ordonnateur feront preuve d'une vigilance accrue lors des déplacements à l'étranger. Il est vivement conseillé de prendre contact avec le service achats de Bordeaux INP avant tout déplacement dans les zones hors Europe, DOM et USA pour connaître les modalités de tarifications.

En cas d'abus avéré ou de cessation de la fonction ouvrant droit à l'octroi d'un moyen de communication, le matériel sera restitué à l'établissement. En cas de changement d'établissement, l'agent peut demander la portabilité du numéro.

## Article 5 – Principes de sécurité

Les principes suivants ont pour objectif de protéger les informations qui constituent le patrimoine immatériel de Bordeaux INP contre toute altération, volontaire ou accidentelle, de leur confidentialité, intégrité ou disponibilité. Tout manquement aux règles qui régissent la sécurité des systèmes d'information est en effet susceptible d'avoir des impacts importants (humains, financiers, juridiques, environnementaux, atteintes au fonctionnement de l'organisme, au potentiel scientifique et technique ou à la vie privée).

### Article 5.1 – Règles de sécurité applicables

Bordeaux INP met en œuvre les mécanismes de protection adaptés sur les systèmes d'information mis à la disposition des utilisateurs.

L'utilisateur est informé que les informations d'authentification qui lui sont attribuées

constituent une mesure de sécurité destinée à éviter toute utilisation malveillante ou abusive.

Les niveaux d'accès aux systèmes d'information ouverts à l'utilisateur sont définis en fonction de missions qui lui sont confiées. Il est responsable de l'utilisation des systèmes d'information auxquels il accède avec les droits qui lui sont conférés par le responsable de sa structure. En cas d'évolution de ses missions une nouvelle autorisation est délivrée par le responsable de structure.

La sécurité des ressources mises à la disposition de l'utilisateur impose le respect des règles suivantes :

- **De la part de Bordeaux INP**

- Limiter l'accès aux seules ressources pour lesquelles l'utilisateur est expressément autorisé ;
- Garantir la disponibilité, l'intégrité et la confidentialité des données de l'utilisateur.

- **De la part de l'utilisateur**

- Se conformer aux directives de sécurité concernant les usages :
  - **o** Relatifs à la connexion
    - Appliquer la politique de gestion des mots de passe de Bordeaux INP :
      - Utiliser au moins 8 caractères
      - Utiliser au moins 2 caractères dans 3 des familles suivantes : minuscules, majuscules, chiffres, symboles
      - Mélanger les familles de caractère dans le mot de passe
    - Garder strictement confidentielles ses informations d'authentification ;
    - Ne pas utiliser les informations d'authentification d'un autre utilisateur, ni chercher à les connaître ;
    - Être vigilant sur les applications et équipements informatiques non maîtrisés par Bordeaux INP sur lesquels sont saisies ou enregistrées ses informations d'authentification ;
    - Ne pas masquer sa véritable identité, ne pas usurper l'identité d'autrui, ne pas accéder, tenter d'accéder, supprimer ou modifier des informations qui ne lui appartiennent pas, s'interdire d'accéder ou de tenter d'accéder à des ressources du système d'information, pour lesquelles il n'a pas reçu d'autorisation explicite ;
    - Ne pas se connecter à des sites internet malveillants ;
    - S'engager à ne pas apporter volontairement des perturbations au bon fonctionnement des ressources informatiques et des réseaux que ce soit par des manipulations des matériels ou des logiciels ;
    - S'assurer que son poste de travail est verrouillé en cas d'absence, même momentanée, de son bureau afin de se prémunir contre les actes malveillants et les vols de documents sensibles.
  - o Relatifs aux données et aux documents professionnels :
    - Protéger les informations qu'il est habilité à manipuler dans le cadre de ses fonctions, selon leur sensibilité. Lorsqu'il crée un document, l'utilisateur détermine son niveau de sensibilité et applique les règles permettant de garantir sa protection durant tout son cycle de vie (marquage, stockage, transmission, impression, suppression…) ;
    - N'opérer les sauvegardes de données, les partages d'information, les échanges collaboratifs, que sur des sites hébergés ou faisant l'objet d'une convention signée par Bordeaux INP et dont la sécurité a été vérifiée par celui-ci ;

        - Ne pas utiliser des supports de données (tels que ordinateur, clé USB, CR ROM, etc.) sans respecter les règles de sécurité de Bordeaux INP et s'assurer de leur innocuité en sollicitant le SIM ;
        - Mettre en œuvre un système de sauvegarde manuel lorsque des sauvegardes automatiques ne sont pas prévues ;
        - De la même manière s'assurer que les dispositions contractuelles avec des intervenants extérieurs comportent des clauses rappelant les rôles et les obligations des acteurs concernés.
- Respecter les consignes de sécurité concernant le matériel ou les logiciels :
    - Ne pas modifier les paramétrages du poste de travail ;
    - Ne pas installer, télécharger ou utiliser des logiciels ou progiciels dont les droits de licence n'ont pas été acquittés, ou ne provenant pas de sites de confiance, ou sans autorisation de son responsable de structure ;
    - Ne pas copier, modifier ou détruire des logiciels de Bordeaux INP ;
    - Respecter les dispositifs mis en place par Bordeaux INP pour lutter contre les virus et les attaques par programmes informatiques ;
    - Utiliser les moyens de protection mis à disposition contre le vol (câble antivol, rangement dans un tiroir fermé à clé, etc.) ou pour garantir la protection des équipements mobiles et des informations qu'ils contiennent (ordinateur portable, disque dur, clé USB…) ;
    - Ne pas désactiver, ni altérer le fonctionnement ou désinstaller l'outil de cryptage lorsqu'il a été installé par Bordeaux INP ;
    - Adapter la sécurité (physique ou logique) des équipements nomades en fonction de la sensibilité de l'information qu'ils traitent et stockent.
- **Signaler le plus rapidement possible au responsable de la sécurité des systèmes d'information tout logiciel ou dispositif suspect ainsi que toute perte, tout vol ou toute compromission suspectée ou avérée d'un équipement stockant des données professionnelles ou de ses informations d'authentification.**

### Article 5.2 – Mesures de contrôle de la sécurité

L'utilisateur est informé que :

- Bordeaux INP peut intervenir (y compris à distance) sur les ressources mises à sa disposition pour effectuer une maintenance corrective, curative ou évolutive.
- La maintenance à distance de son poste de travail est réalisée avec information préalable.
- Toute information bloquante ou générant une difficulté technique pour le système sera isolée et/ou supprimée.
- Des systèmes automatiques de filtrage permettant de diminuer les flux d'information et d'assurer la sécurité et la confidentialité des données sont mises en œuvre.
- Le SIM dispose d'outils techniques pour procéder aux investigations et au contrôle de l'utilisation des systèmes informatique mis en place.

## Article 6 – Traçabilité

Bordeaux INP informe l'utilisateur que le système d'information est surveillé et contrôlé dans le respect de la législation applicable, à des fins de traçabilité réglementaire ou fonctionnelle, d'optimisation, de sécurité, de détection des abus et fraudes (notamment fraude aux examens, détournement de finalité des applicatifs de gestion…).

Le SIM opère, sans avertissement, les investigations nécessaires à la résolution des dysfonctionnements du système d'information ou de l'un de ses composants. Ils

s'appuient pour ce faire, sur des fichiers de journalisation (appelés également « traces », « journaux » ou « logs ») qui recensent toutes les connexions et tentatives de connexions au système d'information. Ces fichiers comportent au minimum les données suivantes : date, identifiant et type d'événement.
Ces fichiers de journalisation sont conservés douze mois conformément à la réglementation.

## Article 7 – Respect de la propriété intellectuelle

Bordeaux INP rappelle que l'utilisation de ses ressources informatiques implique le respect de ses droits de propriété intellectuelle ainsi que ceux de ses partenaires, et plus généralement de tout tiers titulaire de tels droits.

En conséquence, chaque utilisateur doit :

- utiliser des logiciels dans les conditions des licences souscrites,
- ne pas reproduire, copier, diffuser, modifier ou utiliser les logiciels, bases de données, pages web, textes, images, photographies ou toutes autres créations protégées par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits.

## Article 8 – Respect du Règlement Général de Protection des Données (RGPD)

L'utilisateur est informé de la nécessité de respecter les dispositions légales en matière de traitement des données à caractère personnel, conformément au RGPD et à la loi n°78-17 du 6 janvier 1978 dite « Informatiques et Libertés » modifiée.

Ces dispositions s'appliquent à toute création de fichiers comprenant des informations à caractère personnel et aux demandes de traitement afférent, y compris lorsqu'elles résultent de croisement ou d'interconnexion de fichiers préexistants.

En conséquence, tout utilisateur souhaitant procéder à une création ou à un traitement nouveau devra en informer préalablement le délégué à la protection des données qui prendra les mesures nécessaires au respect des dispositions légales.

Tout projet de transfert de données à caractère personnel vers des partenaires extérieurs doit être soumis, après accord du responsable de la structure, à l'avis du DPD**.**

La communication de données à caractère personnel doit être sécurisée, c'est-à-dire que la confidentialité, l'intégrité et l'authenticité des informations doivent être assurés.

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 des systèmes d'information.
Ce droit s'exerce auprès du directeur général de Bordeaux INP – Avenue des facultés – CS 60099 – 33405 TALENCE Cedex. Le délégué à la protection des données (dpd@bordeaux-inp.fr ) est informé par transmission d'une copie de toute demande d'accès, de rectification et d'opposition à l'utilisation des données personnelles.

## Article 9 – Respect du droit à l'image

L'utilisateur autorise Bordeaux INP à utiliser sa photographie d'identité pour la création

de sa carte multiservice, l'élaboration des trombinoscopes (papier et en ligne) ou de l'annuaire.

Il peut exercer son droit de retrait en ligne, sauf en ce qui concerne la carte multiservices, par courrier électronique auprès de dpd@bordeaux-inp.fr.

## Article 10 – Limitation des usages et sanctions

L'utilisateur est tenu de respecter la réglementation applicable et l'ensemble des règles définies dans la présente charte.

Le non-respect de ces règles pourra donner lieu, indépendamment à d'éventuelles actions civiles et/ou pénales, à la suspension temporaire de l'accès au système d'information de Bordeaux INP ainsi qu'à d'éventuelles poursuites disciplinaires.

## Article 11 – Entrée en vigueur de la charte

La présente charte annule et remplace la précédente charte informatique.
Elle est applicable à compter du 29 juin 2018, date de son approbation par le Conseil d'Administration de Bordeaux INP.
Les modifications approuvées par le CA du 25 septembre 2020 entrent en vigueur le 1er octobre 2020.

## Principaux textes de référence applicables

- Règlement européen (UE) 2016/679 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
- Loi du 29 juillet 1881 modifiée sur la liberté de la presse
- Loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés
- Charte déontologique RENATER (https:www.renater.fr/IMG/pdf/charte_fr.pdf)
- Dispositions pénales
    - Code pénal : articles L.226-16 à 226-24, L3232-1 à 323-1 et L. 335-2 ; R.625-10 0 r625-13
    - Loi n°94-361 du 10 mai 1994 sur la propriété intellectuelle des logiciels
    - Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique
    - Code de la propriété intellectuelle relative à la propriété littéraire et artistique
    - Les dispositions relatives au respect de la vie privée, de l'ordre public, du secret professionnel
    - Les dispositions relatives à la protection du potentiel scientifique et technique de la nation.

# Charte d'utilisation des ressources informatiques de Bordeaux INP par des personnes administrant leur poste de travail

Entre Bordeaux INP d'une part,

et

toute personne qui participe aux missions de formation et de recherche, les personnels enseignants, enseignants-chercheurs, les personnels ingénieurs, administratifs, techniques, ouvriers et de service ayant obtenu l'autorisation d'être administrateur de leur poste, ci-après dénommé « l'utilisateur » d'autre part.

## 1. Préambule

Conscient que certains utilisateurs ont besoin d'administrer leur poste pour des raisons variées, Bordeaux INP peut autoriser, sous certaines conditions, ces utilisateurs à être administrateurs de leur poste de travail.
Cette autorisation est conditionnée par l'engagement de l'utilisateur à respecter la présente charte qui s'inscrit dans la Politique de Sécurité du Système d'Information (PSSI) de l'établissement. Elle doit être explicitement donnée.

La charte informatique de Bordeaux INP doit avoir été visée au préalable par l'utilisateur avant qu'il ne puisse accepter le présent complément.

## 2. Information sur les risques

L'utilisateur qui se sert d'un poste de travail qu'il administre reconnaît qu'il a été informé :

- sur les risques d'être administrateur de son poste :
  - installation de programmes contenant des virus ou chevaux de Troie provoquant une compromission de la machine ;
  - modification de l'identité de la machine sur les réseaux ;
  - impossibilité de remonter à l'origine d'une compromission, d'en connaître l'étendue et d'avoir des précisions sur les dégâts causés en cas de suppression des journaux lors de la dite compromission ;
  - recherche d'informations sur les réseaux à son insu ;
  - installation de services sur des ports sensibles ;
  - attaque profitant de lacunes de configuration ou de mises à jour non effectuées ;
  - possibilité de vol des informations d'autres utilisateurs ayant utilisé le poste ;
  - attaques de type déni de service depuis son poste ;
- sur le risque induit par l'utilisation de périphériques externes ou amovibles de type USB sur sa machine :
  - récupération des informations non cryptées sur un périphérique de stockage externe (même si celles-ci ont été supprimées) ;
  - vol de toutes les informations stockées sur la machine ;

- envoi des informations stockées sur la machine, de toutes les informations saisies au clavier par les utilisateurs du poste et des données transitant sur le réseau ;
- destruction irréversible du poste par un « USB Killer » ;

## 3. Contexte

L'utilisateur comprend et accepte :

- que le Service Informatique Mutualisé de Bordeaux INP n'intervienne pas sur son poste pour des besoins qui ne concernent pas les ressources de l'établissement ;
- la nécessité de configurations particulières pour accéder aux ressources informatiques de Bordeaux INP (impression, dossiers partagés...) ;
- les restrictions d'accès aux données sensibles de l'établissement qu'il peut avoir à partir du poste qu'il administre ;

## 4. Engagements

Afin de limiter les risques, l'utilisateur s'engage à respecter les points suivants :

- Utiliser un compte avec des droits standards (non administrateur) pour son utilisation quotidienne ;
- Utiliser un mot de passe robuste et éviter les mots de passe par défaut ou vides ;
- Installer uniquement des programmes qui servent des objectifs professionnels ;
- Installer des programmes qui proviennent uniquement de sites d'éditeurs ;
- Ne pas laisser autrui utiliser sa machine avec un compte ayant des droits administrateurs ;
- Ne pas installer de services qui rendront son ordinateur vulnérable ;
- Ne pas créer de partage de dossier sur le poste ;
- Prévenir le Service Informatique Mutualisé s'il installe intentionnellement un keylogger ;
- Veiller à déconnecter le wifi de son ordinateur lorsqu'il se connecte en filaire sur une prise réseau ;
- S'interdire de brancher son poste sur un réseau de l'établissement sans l'accord du Service Informatique Mutualisé ;
- Protéger son poste par un pare-feu et un antivirus ;
- Verrouiller son écran lorsqu'il s'éloigne de son poste ;
- Crypter ses informations ;
- Sauvegarder régulièrement ses données importantes.