Sciences Po Bordeaux

Sciences Po Bordeaux

Charte des Usagers des Systèmes d'Information de Sciences Po Bordeaux

ComUE d'Aquitaine

université de BORDEAUX

11 allée

Sciences Po Bordeaux

Sciences Po Bordeaux

Fiche de suivi

VERSION	DATE	REDACTEUR	MODIFICATION
V1.0	12/12/2022	Advens	Création du document
V.1.1	14/03/2023	DSIN	Version validée au CA du 01/02/23

Institut d'Études Politiques de Bordeaux
11 allée Ausone • Domaine universitaire • F-33607 Pessac Cedex
Standard : 05 56 844 252 • Sciencespobordeaux.fr

Introduction

1.1 Objectif

La présente charte a pour objectif de fixer les règles d'utilisation des moyens informatiques mis à la disposition des usagers de Sciences Po Bordeaux.

La charte permet d'exposer aux usagers les principales règles juridiques applicables dans le cadre de l'utilisation des ressources informatiques de l'ensemble des parties prenantes de Sciences Po Bordeaux.

La sécurité et le bon fonctionnement des systèmes d'information de Sciences Po Bordeaux dépendent d'un usage des moyens informatiques et de communications électroniques conforme à leur objet. La présente charte permet de sensibiliser chacun des usagers. Par ailleurs, elle informe ces derniers des sanctions encourues, en cas de non-observation des présentes règles, en accord avec la législation en vigueur.

La présente charte pourra évoluer en fonction du contexte légal et de la Politique de Sécurité des Systèmes d'Information (PSSI).

1.2 Champ d'application

La présente charte est applicable et opposable à l'ensemble des usagers susceptibles de pouvoir accéder au système d'information de Sciences Po Bordeaux permanent ou temporaire, quel que soit son statut. Chaque usager est tenu de respecter cette charte d'utilisation du système d'information.

Le terme « usager » est utilisé pour désigner toute personne utilisant ou ayant accès aux ressources informatiques et téléphoniques de l'établissement, aux réseaux (REAUMUR, RENATER, …) et aux services Internet, comme par exemple :

- Les membres du personnel administratif,
- Les enseignants permanents/titulaires,
- Les enseignants contractuels et vacataires,
- Les enseignants-chercheurs, chercheurs (CNRS, FNSP, …),
- Les chercheurs associés et invités (autres universités, laboratoires, IRD, INRIA, …),
- Les étudiants, étudiants/doctorants ou chercheurs,
- Les hébergés,
- Etc.

Cette charte s'applique notamment à l'ensemble des systèmes d'information (postes de travail, serveurs, téléphones, terminaux des salles en libre-service (travaux pratiques, enseignement, bibliothèque, etc.)) des laboratoires, écoles, instituts, services administratifs, …

La confidentialité d'une information étant indépendante de son support, les règles encadrant l'utilisation et la diffusion d'informations confidentielles s'étendent à tous les moyens de communication, y compris la parole ou les documents papiers.

Il est à la charge de l'usager de veiller à ce que cette charte soit respectée par lui-même et par les autres usagers si un comportement anormal est suspecté.

2 Modalités générales d'application

2.1 Responsabilités des usagers et sanctions encourues

L'usager est responsable de l'usage qu'il fait des ressources de l'établissement mises à sa disposition, dans l'exercice de son activité. Toute l'infrastructure informatique et téléphonique présente et à venir au sein de Sciences Po Bordeaux est dédiée à l'utilisation professionnelle ou pédagogique.

Un usage personnel ponctuel et raisonnable de la messagerie et de l'Internet est néanmoins toléré en aide à la vie privée dès lors qu'il respecte la législation en vigueur et qu'il n'est pas susceptible d'affecter la qualité du service associé. Les informations à caractère privé doivent être clairement identifiées comme telles et porter la mention visible « Privé » ou « Perso » au niveau de la messagerie et des partages.

L'utilisation des ressources informatiques communes et la connexion d'un équipement sur le réseau sont soumises à l'autorisation des administrateurs systèmes et réseaux. Ces autorisations sont strictement personnelles et, en aucun cas, ne peuvent être cédées à un tiers. Elles peuvent être révoquées à tout instant et prendre fin en cas de suspension momentanée ou définitive de l'activité qui les a justifiées.

Ainsi, toute utilisation non conforme aux conditions et limites définies par la présente charte est constitutive d'une faute. En conséquence, le non-respect de la réglementation applicable expose l'usager concerné à des sanctions conservatoires, disciplinaires et/ou à des poursuites judiciaires.

En outre, l'usager s'expose à des sanctions concernant son droit d'utiliser les moyens informatiques et de communication électronique mis à sa disposition. Ces sanctions peuvent consister, notamment, dans le contrôle renforcé, la suspension, le blocage, le retrait et même la suppression pure et simple de son droit d'utiliser tout ou partie de ces moyens.

2.2 Protection des informations confidentielles

L'usager est amené à manipuler des informations confidentielles, notamment (et de façon non exclusive) des informations relatives à l'établissement, aux activités, aux études, à la recherche, aux techniques, savoir-faire, méthodes, projets, logiciels, et/ou brevets, ainsi que les idées afférentes à des domaines développés ou mis en œuvre au sein de Sciences Po Bordeaux.

Ces informations constituent les actifs immatériels de l'établissement, c'est pourquoi des mesures particulières doivent être mises en place pour les protéger.

L'usager s'engage notamment à respecter les règles relatives au secret professionnel. En particulier, l'usager s'engage à ne pas effectuer les opérations suivantes :

- **Envoyer ou soumettre des informations confidentielles**, sous toute forme, à toute personne non habilitée à en avoir connaissance,

- **Utiliser des moyens de stockage ou d'échange publics** pour publier ou échanger des informations confidentielles,

- **Transporter les informations** dans des conteneurs non-chiffrés,
- **Laisser sans surveillance** sur un bureau, une imprimante, un fax, un tableau d'affichage ou en tous lieux accessibles à des personnes non autorisées, des informations confidentielles,
- **Conserver de manière non sécurisée** des documents papier confidentiels ou omettre de les détruire ou broyer avant de les jeter.

L'usager a conscience que le respect des règles de confidentialité ne doit pas se limiter à l'usage des outils informatiques mais qu'il doit s'appliquer à tous les modes de communication (téléphone, mails, visio-conférences, conversations, etc.) et en tous lieux.

En particulier, l'usager doit faire preuve d'une vigilance accrue concernant la confidentialité des informations qu'il consulte ou échange lorsqu'il se trouve dans un lieu public (restaurants, transports en commun, etc.).

Lors de tout échange de données confidentielles avec un tiers, un accord de confidentialité doit être signé.

3 Note d'information aux usagers

3.1 Traçabilité et filtrage

Pour satisfaire aux obligations légales qui lui incombent, tenant à sa capacité à apporter la preuve du bon usage des moyens informatiques et de communication électronique mis à la disposition des usagers et à prévenir tout usage illicite de ces mêmes moyens, Sciences Po Bordeaux procède à la mise en place :

- D'outils de traçabilité (journaux de connexions) de l'ensemble des moyens informatiques et de communication électronique permettant de détecter les écarts, abus et comportements suspects sur les systèmes d'information,

- D'outils de filtrage (filtrage des contenus, des URL, etc.) permettant d'analyser les conditions d'utilisation de ces moyens, d'interdire tel ou tel protocole, ou encore de restreindre ou d'interdire l'accès à internet ou à certaines catégories de sites internet.

Tout détournement, altération ou modification de ces outils ou des données recueillies grâce à ces outils est strictement interdit.

3.2 Contrôle et audit

Les opérations de contrôle et d'audit se distinguent des opérations de maintenance en ce qu'elles portent sur la régularité de l'utilisation des moyens informatiques et de communication électronique.

Elles se justifient par les obligations incombant à l'établissement qui est soumis, de par son activité, à une obligation générale de sécurité, en application des dispositions du Code pénal relatives aux atteintes aux systèmes de traitement automatisés de données, et du « Règlement Général sur la Protection des Données ».

Sciences Po Bordeaux dispose également d'un pouvoir de contrôle de l'activité des usagers et, en particulier, le respect par ces derniers de la présente charte. L'utilisation des moyens informatiques et de communication électronique pourra faire l'objet d'une surveillance, afin de détecter toute utilisation non conforme, d'optimiser cette même utilisation ou encore de mener des analyses statistiques.

L'établissement se réserve notamment le droit de :

- Vérifier le trafic informatique entrant et sortant, ainsi que le trafic transitant sur le réseau interne,

- Diligenter des audits pour vérifier que les consignes d'usage et les règles de sécurité et de sûreté sont appliquées sur les ressources du système d'information,

- Contrôler l'origine licite des logiciels installés ou utilisés,

- Conserver des fichiers de journalisation des traces en fonction des besoins propres de chaque système d'information,

- **Transmettre aux autorités judiciaires** sur requête tout ou partie des enregistrements disponibles.

En outre, en cas d'incident, Sciences Po Bordeaux se réserve le droit de :

- **Surveiller le contenu des informations** qui transitent sur son système d'information,
- **Vérifier le contenu des supports numériques** des ressources du système d'information attribuées aux usagers,
- **Procéder à toutes copies utiles** pour faire valoir ses droits.

4 Règles d'utilisation des ressources

4.1 Le poste de travail et l'accès au système d'information

Dans le cadre général de ses activités, l'usager s'engage à respecter les règles d'usage des outils informatiques.

L'usager s'engage à :

- ☑ Appliquer les recommandations particulières de sécurité de l'entité à laquelle il appartient,
- ☑ Prendre toutes les précautions nécessaires pour protéger les équipements mobiles, fixes et accessoires qui lui sont affectés (utilisation du câble antivol pour les portables, utilisation de moyen de transport discrets, etc.),
- ☑ Choisir des mots de passe sûrs (respectant les règles de la PSSI) garder secrets ses mots de passe et ne jamais les diffuser à quiconque, y compris aux administrateurs informatiques, à ses collègues ou aux responsables hiérarchiques. L'utilisation de coffre-fort est recommandée pour stocker ses mots de passe,
- ☑ Faire valider auprès de la DSIN toute installation d'un nouveau périphérique ou logiciel,
- ☑ Signaler, dans les plus brefs délais, tout incident de sécurité avéré ou soupçonné (incident technique, malveillance, fraude, vulnérabilité ou faille de sécurité),
- ☑ En cas de perte ou de vol d'un équipement informatique, informer le plus rapidement possible son responsable hiérarchique et la DSIN,
- ☑ Se connecter uniquement aux réseaux Wifi autorisés, et à ne pas utiliser les prises réseaux sauf accord de la DSIN.

L'usager s'engage à ne pas :

- ☒ Ajouter ou installer des équipements, des logiciels ou progiciels non autorisés par l'établissement, sous toutes formes,
- ☒ Ajouter ou installer des équipements, des logiciels ou progiciels sans disposer d'une licence adéquate pour une utilisation professionnelle ou pédagogique (i.e. licence appartenant à Sciences Po Bordeaux),
- ☒ Profiter des privilèges spéciaux qui lui sont accordés sur le système d'information à des fins non légitimes, en les détournant de leur finalité,
- ☒ Masquer sa véritable identité ou usurper l'identité d'autrui, par quelque moyen que ce soit (sauf dans le cadre de sa mission, sur validation hiérarchique),
- ☒ Quitter tout poste de travail utilisé sans se déconnecter ou sans le verrouiller, sauf évacuation d'urgence,

- ☒ Tenter de lire, modifier, copier ou détruire les données dont il n'a pas la responsabilité sauf autorisation du propriétaire,

- ☒ Faciliter l'intrusion directement ou indirectement dans le système d'information en introduisant des failles de sécurité quelconques ou des virus informatiques,

- ☒ Mettre à disposition d'usagers non autorisés un accès aux systèmes ou aux réseaux, quel que soit le type de moyen employé.

4.2 Les règles de stockage

L'usager est responsable de la pérennité de ses données, de ses fichiers et de l'intégrité de son espace de travail.

L'usager s'engage à :

- ☑ Stocker tous les fichiers en rapport avec son activité dans les répertoires mis à disposition des usagers, sur le réseau. Ceux-ci sont régulièrement sauvegardés et leur sécurité est assurée,

- ☑ Stocker ses données exclusivement personnelles dans un dossier renommé « Personnel » ou « Perso ». Les usagers sont informés qu'aucune mesure de sauvegarde n'est prise vis-à-vis de ce répertoire. L'usage de ce répertoire doit être exceptionnel et demeurer raisonnable en termes de taille et de nature des fichiers stockés,

- ☑ Détruire son ou ses répertoires privés à son départ définitif de Sciences Po Bordeaux. S'il ne l'a pas fait, la DSIN se réserve le droit de les supprimer sans préavis.

L'usager s'engage à ne pas :

- ☒ Conserver ses données professionnelles sur des médias amovibles (clé USB, disque dur, etc.) non chiffrés et non validés par la DSIN,

- ☒ Gaspiller volontairement les ressources communes (espace disque, impressions, occupation des postes de travail, transferts réseaux, occupation de serveurs distants, etc.).

4.3 La messagerie

Le système de messagerie, comme tout système informatique de l'établissement, est destiné à un usage professionnel ou pédagogique. Un usage exceptionnel dans le cadre des nécessités de la vie courante et familiale est toléré, à condition que cette utilisation n'affecte ni les performances du système ni la bonne exécution du contrat qui lie l'usager à Sciences Po Bordeaux.

L'usager s'engage à :

- ☑ Restreindre la diffusion de son adresse mail aux contacts du cadre professionnel ou pédagogique légitimes afin de limiter les problèmes de pollution des systèmes de messagerie,
- ☑ S'il fait usage de la messagerie à titre personnel, inscrire la mention « [PERSO] » dans l'objet du message et supprimer, dans le corps, toute mention relative à l'établissement ou toute autre indication qui pourrait laisser croire que le message est rédigé par l'usager dans le cadre de l'exercice de ses activités,
- ☑ Chiffrer toute donnée sensible avant envoi via la messagerie,
- ☑ Accepter l'existence d'un système automatisé de détection et/ou de rejet des courriels commerciaux non sollicités ("pourriels" ou "spams"), ainsi que des courriels identifiés comme vecteur de virus informatiques,
- ☑ Détruire ses mails « [PERSO] » avant son départ de l'établissement, s'il ne le fait pas, la DSIN se réserve le droit de supprimer l'intégralité de la messagerie sans préavis,
- ☑ Utiliser des outils dédiés (serveurs de listes, ou outil de mailing) pour effectuer les envois groupés dans le cadre de ses activités,
- ☑ Utiliser les listes de diffusion mises à la disposition des usagers de manière raisonnée, légitime et adaptée.

L'usager s'engage à ne pas :

- ☒ Envoyer ou recevoir des messages dans le cadre institutionnel ou professionnel depuis ou à partir de ses adresses de messagerie personnelles,
- ☒ Envoyer des informations confidentielles dans le corps d'un message. Une pièce jointe chiffrée avec l'aide d'une solution autorisée par la DSIN doit être utilisée pour les échanges confidentiels.

4.4 Internet et les outils de communication associés

Sciences Po Bordeaux ne pourra être tenue responsable du contenu des sites visités par l'usager, en dehors de son activité, ni des éventuelles compromissions ou mises en cause qui pourraient avoir lieu suite à la visite de ces sites.

L'usager s'engage à :

- ☑ Ne consulter et n'utiliser que les sites Internet, les forums de discussion ou autres outils de communication utilisant Internet, présentant un lien direct et nécessaire avec son activité,
- ☑ Faire preuve de vigilance vis-à-vis des informations en provenance d'Internet et vérifier leur exactitude avant toute prise de décision importante. D'une manière générale, l'usager doit être vigilant par rapport aux sites qu'il consulte, et il ne doit pas visiter un site si un doute subsiste concernant sa réputation,
- ☑ Accéder de manière responsable à des flux multimédias n'ayant pas de liens avec l'activité (web radios, streaming, etc.) quand ceux-ci sont autorisés.

L'usager s'engage à ne pas :

- ☒ Consulter, télécharger ou propager des informations (textes, images, sons) à caractère illégal, injurieux, raciste, diffamatoire, harcelant, obscène ou menaçant,
- ☒ Télécharger (envoyer ou réceptionner) des fichiers volumineux à des fins personnelles,
- ☒ Utiliser un logiciel de messagerie instantanée non autorisé par la DSIN.

4.5 Les communications virtuelles et les réseaux sociaux

L'usager désirant participer en tant que contributeur à une communauté virtuelle ayant un rapport avec son activité doit obtenir l'autorisation formelle de son responsable. L'usager reste responsable du contenu qu'il diffuse.

L'usager s'engage à :

- ☑ Faire valider par son supérieur hiérarchique et/ou par le service communication toute information publiée à l'extérieur et dont le contenu est relatif à l'établissement.

L'usager s'engage à ne pas :

- ☒ Permettre à des tiers non autorisés d'avoir accès à des informations confidentielles ou à propos du système d'information de l'établissement,
- ☒ Publier des informations qui pourraient nuire aux intérêts de Sciences Po Bordeaux (propos diffamatoires, etc.).

L'attention de l'usager est attirée sur le fait que la plupart des réseaux sociaux ou outils de communication sur Internet gardent une trace des connexions. Dans certains cas, ces sites identifient précisément la provenance du visiteur et son identité électronique, pouvant directement mettre en cause l'établissement.

4.6 L'accès à distance

Sciences Po Bordeaux met à la disposition des usagers un système de connexion à distance au système d'information.

L'usager s'engage à :

- ☑ Se conformer aux mêmes règles que celles qu'il suit lorsqu'il accède aux ressources informatiques depuis les locaux de l'établissement, notamment lors de l'échange de données ou du dépôt de fichiers,
- ☑ Être conscient qu'il est plus exposé que les autres usagers à certains risques, lorsqu'il est en dehors des locaux, et que la sécurité de l'information de l'établissement dépend fortement de son comportement.

L'usager s'engage à ne pas :

- ☒ Contourner ou essayer de contourner les mesures de protection mises en place,
- ☒ Apporter des changements à la configuration de l'outil d'accès à distance sans l'accord préalable de la DSIN.

4.7 La téléphonie

L'établissement met à disposition de certains de ses usagers des téléphones. Ces téléphones, comme tout système de Sciences Po Bordeaux, sont destinés à un usage professionnel ou pédagogique. Un usage exceptionnel dans le cadre des nécessités de la vie courante et familiale est toléré, à condition que cette utilisation n'affecte ni les performances du système ni la bonne exécution de ses missions.

Certains téléphones offrent des possibilités d'accès à Internet. Dès lors qu'ils sont connectés au système d'information, ces téléphones sont de fait soumis aux mêmes règles de sécurité que les autres composants du système d'information. Par conséquent, toutes données sur le périphérique mobile appartenant à Sciences Po Bordeaux ou à des tiers, doivent obligatoirement être stockées de façon chiffrée.

De plus, les usagers doivent respecter les règles éditées dans la PSSI de Sciences Po Bordeaux en ce qui concerne l'utilisation des téléphones fixes et mobiles.

4.8 Le respect des lois en vigueur

L'établissement est en droit de révéler aux autorités les activités illicites éventuellement perpétrées en son sein. L'énumération ci-dessous, non limitative, pourra être complétée, après consultation des instances représentatives du personnel, en fonction des évolutions techniques ou légales futures.

L'usager s'engage à :

- ☑ S'assurer de posséder les droits (ou autorisations) concernant le chargement, le stockage, la publication, la diffusion ou la transmission des éléments protégés par les lois sur la propriété intellectuelle. L'usager s'interdit de solliciter l'envoi par des tiers, en pièces jointes de tels fichiers,

- ☑ Dans le cas où un usager est amené à mettre en place un traitement de données à caractère personnel contenues ou appelées à figurer dans des fichiers, il doit prendre toutes les mesures nécessaires afin que ce traitement soit conforme aux dispositions de la loi du 6 janvier 1978, modifiée par la loi du 20 juin 2018 et l'ordonnance de réécriture du 12 décembre 2018, relative à l'informatique, aux fichiers et aux libertés et au Règlement General de Protection des Données qui est entré en application le 25 mai 2018,

- ☑ Respecter les obligations de réserve, de discrétion et de secret professionnel.

L'usager s'engage à ne pas :

- ☒ Télécharger, stocker, publier, diffuser ou transmettre de documents dont le contenu porte atteinte aux bonnes mœurs et à l'honneur, à caractère pornographique ou véhiculant des idées ou des valeurs contraires à la morale ou interdites par la loi, notamment l'envoi de messages ou la consultation de sites racistes, révisionnistes, pédophiles, prônant la discrimination sur base du sexe, de l'âge, des origines supposées, de l'orientation sexuelle, du handicap, de la religion ou des convictions politiques ou syndicales d'une personne ou d'un groupe de personnes.

Une attention particulière doit être portée sur les règles de confidentialité et les données personnelles. En effet, il est illicite, sauf accord explicite du propriétaire, de prendre connaissance d'informations détenues par d'autres usagers même si ceux-ci ne les ont pas protégées. Cette règle s'applique également aux échanges privés de type courrier électronique dont l'usager n'est destinataire ni directement, ni en copie.

De plus, si dans l'accomplissement de son activité, l'usager est amené à manipuler des données personnelles, il devra s'assurer que les règles de base de la sécurité de l'information (Disponibilité, Intégrité, Confidentialité) soient observées en vérifiant que :

- Le stockage soit sécurisé,
- Le traitement soit autorisé, après une consultation de son responsable hiérarchique et/ou du Délégué à la Protection des Données (DPO).

Enfin, le respect de la législation sur la propriété intellectuelle est également objet des contrats de travail de Sciences Po Bordeaux en vigueur.

4.9 Les administrateurs

Pour des nécessités de maintenance et de gestion technique, l'utilisation des ressources matérielles ou logicielles ainsi que les échanges via le réseau peuvent être analysés et contrôlés par les administrateurs systèmes et/ou réseaux dans le respect de la législation applicable, notamment du Règlement Général sur la Protection des Données, et de la jurisprudence.

L'administrateur s'engage à :

- ☑ Accéder, sur les systèmes ou les réseaux qu''il administre, aux informations nécessaires à des fins de diagnostic et d'administration des systèmes ou des réseaux en respectant scrupuleusement la confidentialité de ces informations et en s'efforçant de ne pas les altérer,
- ☑ Prioriser, au-dessus de toutes les autres tâches liées au numérique, celles nécessaires au maintien des défenses informatiques destinées à protéger les actifs de Sciences Po Bordeaux par le blocage, la réduction ou l'éradication des attaques informatiques détectées ou redoutées,
- ☑ Maintenir les systèmes dont il a la responsabilité au meilleur niveau de protection par la mise en œuvre des correctifs de sécurité fournis,
- ☑ Respecter les règles de confidentialité, en se limitant à l'accès aux informations strictement nécessaires et en respectant le « secret professionnel »,
- ☑ Faire respecter cette charte informatique aux usagers de Sciences Po Bordeaux.

L'administrateur s'engage à ne pas :

- ☒ Entraver les procédures de surveillance des tâches exécutées sur l'infrastructure technique, afin de déceler les violations ou les tentatives de violation de la présente charte,
- ☒ Utiliser ses privilèges sur le système d'information à des fins personnelles,
- ☒ Interrompre les services ou imposer des limitations (débits réseau, impressions, etc.) aux usagers sans aucune raison professionnelle,
- ☒ Utiliser leur compte administrateur sur des équipements personnels.

Sciences Po Bordeaux

5 Engagement personnel

Je soussigné(e)

Nom :

Prénom :

Qualité :

Déclare avoir pris connaissance de la présente Charte des Usagers des Systèmes d'Information de Sciences Po Bordeaux.

A ……le …/…/…

Signature
(A faire précéder de la mention « Lu et approuvé »)

Institut d'Études Politiques de Bordeaux
11 allée Ausone • Domaine universitaire • F-33607 Pessac Cedex
Standard : 05 56 844 252 • Sciencespobordeaux.fr

6 Annexes

6.1 Annexe 1 – Lexique

Dans un souci de clarté, les termes utilisés dans ce document sont explicités dans la suite. Les usagers peuvent contacter le Responsable de la Sécurité des Systèmes d'Information (RSSI) de l'établissement pour toute question complémentaire concernant cette charte.

- **Administrateur** : Personne responsable du bon fonctionnement de tout ou partie du système d'information et ayant des droits supérieurs aux usagers normaux.
- **Confidentialité** : Fait d'assurer que l'information n'est accessible qu'aux personnes autorisées. La confidentialité est une obligation légale pour les données à caractère personnel.
- **Intégrité** : Fait d'assurer que l'information est fiable et ne peut subir aucune altération volontaire ou involontaire.
- **Traçabilité :** Fait d'assurer que les modifications apportées à l'information sont enregistrées et peuvent être analysées dans le futur.
- **Donnée à caractère personnel** : Toute information relative à une personne physique identifiée ou qui peut être identifiée directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.

  Cette définition fait référence au Règlement General sur la Protection des Données (RGPD).
- **Traitement de données à caractère personnel** : Toute opération ou tout ensemble d'opérations portant sur des données à caractère personnel et notamment, la collecte, l'enregistrement, la transmission ou la communication.
- **Information** : Toute donnée appartenant à Sciences Po Bordeaux ou étant en relation avec ses partenaires et ce, indépendamment de son support (papier, informatique, oral).
- **Ressource/actif** : Composant matériel (ordinateur, imprimante, serveur…) ou immatériel (application, base de données, procédures…) contribuant au traitement de l'Information.
- **Spam, pourriel** : Le spam est l'envoi massif, et parfois répété, de courriers électroniques non sollicités, à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact et dont il a capté l'adresse électronique de façon irrégulière.
- **Système d'information** : Ensemble des moyens humains, techniques et organisationnels permettant de créer, de conserver, d'échanger et de partager des informations entre les acteurs interne et externe de l'établissement, quelle que soit la forme sous laquelle elles sont exploitées (électronique, imprimée, manuscrite, vocale, image, …).
- **Usager** : Toute personne autorisée à accéder, utiliser ou traiter des ressources du système d'information de Sciences Po Bordeaux dans le cadre de son activité.
- **DSIN** : Direction des Systèmes d'Information et du Numérique.

6.2 Annexe 2 – Contrôle de l'utilisation des ressources

L'établissement peut être jugé responsable des actes de ses usagers. Pour cette raison, il met en place un contrôle de l'utilisation des différents moyens de communication et d'information mis à la disposition des usagers. Ces contrôles seront révisés régulièrement selon un processus défini dans la Politique de Sécurité du Système d'Information (PSSI).

Conformément aux exigences du droit français dans ce domaine, les restrictions et les surveillances mises en place sont définies ci-après.

Contrôle de l'utilisation

Les solutions de sécurité et les applications mises en œuvre par l'établissement génèrent des enregistrements ou traces utilisés pour le suivi, l'administration et le support des solutions. Ces traces peuvent, de manière exceptionnelle, être utilisées pour effectuer des recherches en cas de suspicion d'une activité malveillante pouvant porter atteinte à Sciences Po Bordeaux.

Une exploitation statistique des enregistrements peut être réalisée sous forme anonyme pour des motifs opérationnels. Elle consiste à établir des statistiques relatives aux connexions et contacts réalisés. Néanmoins, l'établissement peut procéder à des audits à caractère nominatif sur les enregistrements informatiques, suite à un dysfonctionnement, une alerte de sécurité ou une présomption d'utilisation non conforme des moyens informatiques.

Dans ce but, les traces seront conservées pendant une durée d'un an. Elles seront également archivées pendant un an, sur un support indépendant, muni d'un dispositif de traçabilité des consultations, dont l'accès est limité aux autorités judiciaires afin de leur permettre la recherche, la constatation et la poursuite d'infractions pénales.

Conformité poste de travail

Le poste de travail usager constitue un élément clé du réseau de l'établissement. Du fait de l'évolution des menaces et des techniques de protection, le poste de travail est devenu la partie la plus vulnérable. Par ailleurs, c'est aussi la partie la plus difficile à protéger du fait de ses contraintes d'utilisation et d'administration.

Afin de garantir que soit maintenue la conformité aux politiques de sécurité de l'établissement et aux règlementations et normes applicables, l'ensemble des postes de travail présents sur le réseau fait l'objet de contrôles réguliers. A savoir :

- Une vérification de la configuration du poste en matière de sécurité, en particulier : l'autorun désactivé, la mise en veille automatique et la demande du mot de passe lors de la reprise, etc.,
- L'installation des derniers correctifs en matière de sécurité,
- L'activation de l'antivirus et de sa mise-à-jour,
- La présence de logiciels interdits (P2P, torrent, streaming, etc.).

Conformité téléphones mobiles

De par leur nature mobile et la sensibilité des informations qui y sont stockées, les téléphones mobiles représentent une vulnérabilité importante pour la sécurité de l'information.

Afin de garantir la conformité aux politiques de sécurité de l'établissement et aux règlementations et normes applicables, il est fortement conseillé aux usagers bénéficiaires d'appliquer les bonnes pratiques suivantes :

- La mise à jour régulière des systèmes d'exploitation mobile selon les publications du constructeur,
- La restriction de l'accès à la carte SIM (code non trivial), au système d'exploitation mobile (pattern et/ou code non triviaux) et aux applications connectées au système d'Information (login et mot de passe),
- La présence et la mise à jour quotidienne d'une solution antivirus validée par la DSIN,
- La restriction de connexion aux seuls points d'accès sans-fil de confiance,
- L'extrême vigilance des usagers quant à l'installation de logiciels provenant de tierces parties, notamment vis-à-vis des autorisations systèmes accordées aux applications,
- L'installation des logiciels depuis des dépôts reconnus (AppStore, Google Play, etc.).

Système d'authentification et d'habilitations

Les ressources mises à disposition de l'usager suivent une procédure d'habilitation et utilisent des systèmes d'authentification. Ces systèmes conservent des traces enregistrant l'identification de l'usager et la date et l'heure de sa demande d'authentification ou d'usage de ses habilitations.

Protection de la messagerie

La protection de la messagerie repose sur une solution Antivirus et Anti-spam, le contrôle des pièces jointes, le contrôle de la taille des messages, et un système de trace enregistrant, pour chaque message, l'adresse électronique de l'expéditeur, l'adresse électronique du destinataire, la date et l'heure, la taille du message ainsi que les caractéristiques des pièces jointes (le nombre, la taille et le type).

Ce dispositif s'applique à l'intégralité des messages gérés par les systèmes de messagerie de l'établissement.

Protection de l'accès internet

La protection de l'accès Internet repose sur un système de traces (combinaison des pare feux et anti-virus sur le poste de travail), enregistrant pour chaque connexion, l'adresse IP, le site consulté, la date et l'heure de la consultation.

L'établissement se réserve le droit de bloquer à tout moment et sans avertissement préalable l'accès aux sites dont elle juge le contenu manifestement illicite, offensant, sans rapport avec l'activité ou présentant un risque de sécurité

Protection de l'image de marque

La protection de l'image de l'établissement passe par la maîtrise de l'image de marque de Sciences Po Bordeaux sur Internet et en particulier sur les communautés virtuelles et les réseaux sociaux. Des contrôles ponctuels sont mis en œuvre sur les informations publiées à l'extérieur et dont le contenu est relatif à l'établissement.