UNIVERSITÉ DE PAU ET DES PAYS DE L'ADOUR

Charte des usagers du numérique

Approuvée par le conseil d'administration du 20/12/2024

SOMMAIRE

PRÉAMBULE

Le recours exponentiel aux systèmes d'information d'une part et l'accroissement des menaces qui les visent amènent l'État à investir le champ du numérique afin de définir les exigences organisationnelles, techniques ou contractuelles minimales applicables à ces systèmes d'information tout en tenant compte des enjeux de sécurité associés au domaine qu'elles adressent.

Ces exigences visent aussi bien à garantir la protection d'informations hautement sensibles qu'à préserver la continuité de services essentiels au fonctionnement de la nation.

Le décret n° 2019-1088 du 25 octobre 2019, modifié par le décret n° 2022-513 du 8 avril 2022, et la politique de sécurité des systèmes d'information de l'État (PSSIe) définissent le cadre de gouvernance de la sécurité numérique des administrations et établissements publics d'État.

OBJET

Conformément à l'article 8 du règlement intérieur de l'établissement, la présente charte a pour objet de fixer les règles d'usage des moyens numériques de l'UPPA.

PORTÉE

La présente charte a vocation à s'appliquer dans le cadre des usages des différents services numériques de l'établissement.
La présente charte ne porte que sur les services numériques dont l'université est responsable et ne vise donc pas les services numériques qui ne seraient pas validés, créés ou exploités par l'établissement lui-même.
Les services numériques peuvent être gérés directement par l'établissement ou par le biais d'un sous-traitant spécifiquement désigné par l'établissement.

Cette charte est annexée à l'article 8 du règlement intérieur « Charte des usagers du numérique ».

OPPOSABILITÉ

La présente charte est opposable :

- aux AGENTS (enseignants-chercheurs, enseignants du second degré, enseignants associés, attachés temporaires d'enseignement de recherche, doctorants contractuels et vacataires sans discrimination d'heures d'enseignements effectuées dans l'année, personnels administratifs et techniques ou BIATSS) ;
- aux USAGERS de l'établissement, étudiants embauchés ponctuellement par l'établissement, personnels mis à disposition de l'établissement, stagiaires de l'UPPA ;
- à toute personne qui utilise le SI de l'UPPA.

1. DOMAINE D'APPLICATION ET DÉFINITIONS

La présente charte des usagers du numérique présente les bonnes pratiques de sécurité numérique (SécNum). Elle a pour objet de satisfaire à l'obligation d'information de l'université de Pau et des pays de l'Adour et ainsi de formaliser les droits et les obligations des AGENTS au regard des usages du numérique. Elle a pour but d'informer l'ensemble des usagers du numérique de leurs droits et de leurs responsabilités, à l'occasion de l'usage approprié des ressources et des services numériques relevant de l'Université de Pau et des Pays de l'Adour (ci-après dénommée « Université »).

Ces usages comprennent l'ensemble des moyens accordés aux usagers du numérique de l'Université dans l'exercice de leurs missions et activités. Les systèmes d'information comprennent tant les réseaux filaires et sans fil que les applications, outils et services tels que les accès à internet mis à leur disposition.

Le bon fonctionnement des moyens numériques, et notamment du système d'information, suppose la sécurité, la performance des traitements, la conservation des données professionnelles et le respect des obligations légales et réglementaires.

Tout usager du numérique, quel que soit son statut et quels que soient les droits numériques qui lui sont accordés est donc responsable, en tout lieu, de l'usage des moyens numériques, des accès Internet dont il dispose et en particulier de son compte informatique (identifiant + mot de passe).

Ainsi on désignera sous le terme :

- « système d'information » : un ensemble organisé de ressources (acteurs, données, procédures, matériels, logiciels, etc.) permettant d'acquérir, de stocker, de structurer et de communiquer des informations sous forme de textes, images, sons ou de données chiffrées ;
- « le numérique » : il s'agit de l'ensemble des réseaux, des moyens informatiques et de leur documentation pour la pédagogie, la recherche et l'administration. Ces moyens, qui permettent le traitement automatique de l'information et peuvent être accédés à distance, directement ou en cascade à partir du réseau de l'Université ou d'internet. Ils comprennent les systèmes d'exploitation, les logiciels, le web, les bases de données, les différents types de documents, etc. ;
- « services numériques » : la mise à disposition par des serveurs locaux ou distants de moyens d'échanges et d'informations diverses : web, VPN UPPA, messagerie, forum, visioconférence, etc. ;
- « usager du numérique » : la personne ayant le droit d'utiliser les moyens numériques et les services Internet mis à sa disposition par l'Université quel que soit son statut (personnels administratifs, enseignants, étudiants, administrateurs, etc.). Ses droits d'accès sont validés par une autorité d'enregistrement ;
- « poste de travail » : ordinateur portable et ordinateur fixe fonctionnant sous MacOS, Linux et Windows ;
- « terminaux mobiles » : téléphone mobile (smartphone) et tablettes fonctionnant sous Android et iOS.

2. ACCÈS AU RÉSEAU DE L'UPPA

L'Université met à disposition des usagers du numérique un accès à son réseau informatique qui peut être réalisé sur les campus par le biais d'une connexion filaire (Ethernet), d'un accès sans fil (Wi-Fi) ou à distance au travers d'un service sécurisé (VPN[1]) ou en accès public selon le cas.

2.1. Caractère des accès

Le réseau de l'Université donne tant un accès à Internet, qu'aux ressources numériques autorisées dans le cadre des activités et missions de chacun des usagers du numérique.

Il est rappelé que l'utilisation des ressources numériques professionnelles à titre privé est tolérée dans une proportion raisonnable. Ces ressources doivent essentiellement conserver un caractère professionnel en restant vigilant sur les risques suivants :

- saturation des accès mis à disposition ;
- utilisation détournée des ressources numériques professionnelles à titre privé.

2.2. Usage d'Internet et des ressources numériques de l'UPPA

2.2.1. Compréhension du nom de domaine de l'établissement

Le nom de domaine Internet de l'établissement est « univ-pau.fr ». Il est utilisé pour construire les adresses électroniques et les adresses des sites et applications web. Le nom de domaine permet d'accéder aux services de l'établissement.

Dans une adresse Internet ou URL, il se présente toujours sur la forme (le / à la fin est important) : **.univ-pau.fr/**

Par exemple :

- https://www**.univ-pau.fr/**
- https://moncompte**.univ-pau.fr/**
- https://nuage**.univ-pau.fr/**
- …

Dans une adresse électronique, il se présente toujours sous la forme : **@univ-pau.fr** ou **@etud.univ-pau.fr**. Les adresses électroniques se doivent se présenter sous la forme **prenom.nom@univ-pau.fr**.

L'utilisation de l'adresse sous la forme login@univ-pau.fr est très fortement déconseillée.

2.2.2. Respect de la législation

- Il est rappelé à l'usager du numérique qu'il est soumis à l'ensemble des règles de droit en vigueur (Chapitre VI), ce qui implique :
- Le téléchargement et l'utilisation de fichiers, notamment logiciels, images, vidéo ou audio doivent s'effectuer dans le respect du droit de la propriété intellectuelle,

1 VPN (Virtual Private Network) : service permettant de créer une connexion réseau directe entre un ordinateur connecté à Internet et le réseau UPPA. Il utilise un mécanisme de chiffrement qui garantit la confidentialité des échanges.

- La consultation volontaire ou répétée de sites répréhensibles ou non appropriés (par exemple des sites pornographiques) depuis le réseau de l'université est proscrite. Seule la consultation de tels sites justifiée par des travaux de recherche scientifique ou dans le cadre de procédures juridiques peut déroger à la présente charte.

2.2.3. Journalisation des accès réseau

L'activité numérique de chaque usager du numérique est enregistrée dans des fichiers conservés au sein de l'Université. Ces fichiers appelés « fichiers de journalisation » peuvent être notamment utilisés à des fins d'analyse en cas de cyberattaque, d'incident de sécurité du numérique ou de réquisition judiciaire.

Dans la mesure où l'Université fournit un accès à Internet, elle est dans l'obligation légale de mettre en place un système de journalisation des accès à son réseau.

Les données issues de cette journalisation sont traitées dans le respect de la réglementation en matière de protection des données à caractère personnel comme décrits au Chapitre VI.

2.2.4. Responsabilité de l'UPPA

L'Université est responsable du maintien d'un niveau de bon fonctionnement de son réseau. Pour ce faire, et pour garantir une bonne fluidité et une disponibilité, l'Université peut :

- Filtrer ou interdire l'accès à certains sites,
- Limiter le téléchargement de certains fichiers trop volumineux,
- Bloquer le téléchargement de fichiers présentant un risque pour la sécurité des systèmes d'information, tel que les virus, code malveillant ou programmes espions,
- Procéder à des statistiques pseudonymisées mesurant le trafic, incluant les sites visités ou les durées de connexions.

2.3. Sécurité

2.3.1. Responsabilité individuelle des usagers du numérique

L'usager du numérique, par le respect des règles de sécurité formulées notamment dans la présente charte, et par sa vigilance, est le premier niveau de sécurité de l'Université.

La majorité des attaques informatiques passent par des actions non sécurisées des usagers du numérique, par le biais de courriels ou clés USB piégés, de l'installation de logiciels ou de la consultation de sites malveillants.

Par conséquent, tout usager du numérique assume la responsabilité des ressources numériques qui lui sont confiées par l'Université. En cas de non-respect des règles de sécurité de la présente charte, l'usager du numérique pourrait s'exposer à des sanctions disciplinaires voire pénales.

Tous les personnels de l'Université en charge du pilotage, de l'administration, de la sensibilisation ou encore de la formation des usagers du numérique, contribuent à la prise en compte des règles de la présente charte.

2.3.2. Respect des règles de sécurité

L'usager du numérique s'engage :

- • À ne pas nuire volontairement au bon fonctionnement des ressources numériques de l'UPPA,

- à ne pas procéder à des modifications et des manipulations non prévues des logiciels fournis par l'UPPA ;
- à ne pas télécharger et installer ou utiliser des logiciels ou progiciels dont les droits de licence n'ont pas été acquittés ou qui proviendraient de sites douteux ;
- à ne pas introduire volontairement sur les systèmes de l'UPPA des logiciels malveillants connus sous les noms génériques de virus (malware), cheval de Troie (trojan), rançongiciel (ransomware), bombes logique, etc ;
- à rester vigilant vis-à-vis quant à la provenance et à l'utilisation de supports amovibles tels que les clés USB ou les disques amovibles (exemple : ne pas utiliser un support trouvé dans une salle ou sur le parking) ;
- à ne pas créer des réseaux, des serveurs et des connexions à distance sur les postes de l'Université, reliant Internet au réseau de l'UPPA de manière non maîtrisée par les administrateurs des Systèmes d'Information.

2.3.3. Besoins spécifiques

Tout besoin spécifique, interdit par la présente charte, doit faire l'objet d'une demande motivée et approuvée hiérarchiquement. L'usager adressera, dans un délai raisonnable, la demande à son informaticien de Proximité qui transmettra à la Sécurité du Numérique (SécNum).

2.4. Autres matériels connectés

Il est rappelé que les règles ci-dessus concernent tout type de matériel fourni par l'Université et dès lors qu'il se connecte au réseau local, en filaire ou via une connexion sans fil : ordinateur fixe, ordinateur portable, tablette, téléphone mobile, etc.

Tout autre matériel personnel, ne provenant pas de l'établissement peut bénéficier d'une connexion qui permet l'accès à Internet et aux ressources locales selon les habilitations de l'usager du numérique.

3. COMPTE UTILISATEUR ET ACCÈS AUX SI DE L'UPPA

3.1. Respect des droits d'accès

Lors de son arrivée à l'Université, chaque usager du numérique dispose d'un compte, appelé « compte informatique », matérialisé par un identifiant et un mot de passe :

- l'identifiant est défini automatiquement ;
- l'usager du numérique doit créer son mot de passe dans l'application https://moncompte.univ-pau.fr.

Le mot de passe est strictement personnel et ne peut en aucun cas être communiqué à un tiers.

L'usager du numérique est donc responsable de son compte informatique et de l'utilisation qui peut en être faite.

Le compte informatique peut être limité ou suspendu à tout moment notamment en cas d'incident de sécurité (par exemple, compromission du compte informatique ou comportement non conforme à la présente charte).

Les autorités d'enregistrement des comptes informatiques définissent les droits d'accès du compte informatique en fonction du rôle de l'usager du numérique ou de sa mission. Ces droits d'accès prennent

fin automatiquement en cas de cessation d'activité, même provisoire de l'usager du numérique ou de non-respect des règles définies dans la présente charte.

L'autorité d'enregistrement des comptes informatiques est habilitée à gérer les demandes de prolongation.

Toute demande liée au compte informatique doit être formulée par l'usager du numérique depuis l'application https://moncompte.univ-pau.fr.

L'usager du numérique s'engage par ailleurs:

- à ne pas accéder à des ressources du système d'information sans y avoir été explicitement autorisé (respect de la confidentialité selon la politique de sécurité de l'information) ;
- à ne pas chercher à connaître le mot de passe du compte informatique d'un autre usager du numérique ;
- à ne pas faire usage des droits d'accès d'une tierce personne, ou usurper une identité d'une tierce personne ;
- à ne pas intercepter des communications entre tiers ;
- à ne pas masquer sa propre identité.

L'usager du numérique signale immédiatement, à son informaticien de proximité ou au correspondant sécurité du système d'information (CSSI) dont il dépend, toute faille de sécurité ou toute possibilité d'accès non contrôlé qu'il découvre.

La liste des CSSI est publiée sur l'intranet de l'Université.

3.2. Authentification

Lors de la connexion au SI, il est nécessaire de s'identifier et de valider cette identité : il s'agit de l'authentification.
En complément du paragraphe III.1, le mécanisme d'authentification s'appuie sur le mot de passe.
L'authentification est effectuée à la page dédiée à l'adresse Internet (URL) : https://sso.univ-pau.fr/cas/

3.3. Protection des mots de passe et des droits d'accès

Le seul moyen autorisé pour modifier son mot de passe est d'accéder à l'application dédiée à l'adresse Internet (URL) : https://moncompte.univ-pau.fr/.

Le compte informatique doit être utilisé uniquement pour s'authentifier sur les applications fournies par l'établissement : liste disponible sur https://mesapplications.univ-pau.fr/.

L'usager du numérique se doit de choisir un mot de passe robuste :

- il applique les règles de complexité de mot de passe proposées dans l'application https://moncompte.univ-pau.fr/ ;
- il effectue le renouvellement de son mot de passe **tous les ans** ;
- il limite l'utilisation de son mot de passe aux sites web du domaine « univ-pau.fr » (liste disponible sur https://mesapplications.univ-pau.fr/) ;
- il respecte la séparation des usages professionnels et ses usages privés ;
- il garde strictement confidentiels son ou ses mots de passe en les stockant dans un conteneur sécurisé ;

- il ne les communique jamais à personne sous quelque forme que ce soit ;
- il ne les écrit pas sur papier, ni dans un fichier informatique non-chiffré ;
- il ne les utilise pas dans des environnements exposés : wifi public, cybercafé, visibilité de l'écran et du clavier par d'autres personnes (l'utilisation d'un filtre de confidentialité est fortement recommandée).

3.4. Confidentialité des informations

L'usager du numérique est tenu de protéger l'information qu'il est amené à créer ou à manipuler dans le cadre de ses fonctions. Les bonnes pratiques consistent à :

- définir le niveau de sensibilité de l'information selon la politique de sécurité de l'information ;
- s'assurer d'un marquage adapté ;
- s'assurer des conditions de stockage conformes au niveau de sensibilité de l'information ;
- utiliser des moyens de transmission chiffrés, notamment avec Internet et la messagerie électronique.

Quelle que soit la forme de l'information, celle-ci doit toujours être sécurisée : sous clé, sur un poste verrouillé, un dispositif de stockage chiffré, etc.

Pour respecter la séparation des usages professionnels et privés, l'usager du numérique utilise son courriel UPPA pour les sites en rapport avec son activité professionnelle.

De plus, l'usager du numérique s'engage à respecter la confidentialité des informations professionnelles. Il s'interdit ainsi de publier sur Internet ou les réseaux sociaux :

- des informations sensibles ou confidentielles ;
- des informations non maîtrisées par la direction de la communication de l'université ;
- des informations pouvant nuire à la réputation de l'université.

4. MESSAGERIE ÉLECTRONIQUE DE L'UPPA

4.1. Mise à disposition d'une adresse de messagerie électronique (courriel ou mél)

À partir de son compte utilisateur et selon ses droits, l'usager du numérique dispose d'une adresse électronique qui lui est propre dans le domaine « univ-pau.fr » appelée adresse électronique institutionnelle. Lors de la création de cette adresse, plusieurs possibilités sont proposées : il est recommandé de privilégier le format prénom.nom@univ-pau.fr quand il est disponible. L'ajout d'une adresse de messagerie non proposée initialement est possible sur demande.

Les informations à caractère professionnel, émanant de l'administration seront diffusées exclusivement sur l'adresse électronique institutionnelle.

La messagerie électronique est un outil de travail destiné à des usages professionnels.

Tout message sera réputé professionnel sauf s'il comporte la mention particulière « privé » ou « personnel », explicitée dans son objet indiquant son caractère privé ou s'il est stocké dans un dossier de messagerie intitulé « privé » ou « personnel ». L'usager du numérique est responsable de ses données à

caractère privé et il lui appartient de les détruire au moment de son départ. L'usager du numérique ne doit pas transformer de messages de nature professionnelle en correspondance privée.

Les mesures de conservation des données professionnelles, notamment pour garantir la continuité de service, sont définies avec la Direction du Numérique de l'UPPA.

Si l'usager du numérique s'aperçoit que le mot de passe de son compte utilisateur a été dérobé ou qu'un tiers a accès à sa messagerie électronique, il doit modifier immédiatement le mot de passe et le signaler en ouvrant un ticket d'assistance (https://assistance.univ-pau.fr/).

Les usagers du numérique sont informés que l'Université se réserve le droit de retenir, d'isoler ou de supprimer tout message à l'aide de moyens automatisés et ce, sans que ces messages aient été nécessairement ouverts, afin d'éviter la propagation de logiciels malveillants.

D'une manière générale les usagers du numérique sont informés que tout message bloquant ou présentant une difficulté technique d'acheminement à son destinataire peut être détruit sur décision d'une autorité de sécurité numérique (Président, DGS ou VP Numérique).

4.2. Contenu des échanges par mail

Les informations échangées par voie électronique avec des tiers peuvent, au plan juridique, être utilisées à des fins probatoires.

L'usager du numérique est donc informé que le courriel pourrait avoir valeur de preuve en cas de contentieux.

L'usager du numérique doit, en conséquence, être prudent sur :

- la nature des informations qu'il échange par voie électronique au même titre que pour les courriers au format papier ;
- les informations reçues (désinformation, virus, tentative d'escroquerie, chaînes, hameçonnage, etc.) ;
- le fait de ne pas ouvrir de fichiers en provenance d'un expéditeur inconnu, en particulier les fichiers compressés ou exécutables.
- Le fait de ne pas ouvrir de fichiers en provenance d'un expéditeur inconnu, en particulier les fichiers compressés ou exécutables.

4.3. Listes de diffusion

L'établissement opère et met à la disposition des AGENTS et des USAGERS de l'établissement des listes de diffusion qui permettent de réaliser des activités de communication.

Ces listes adressent différentes populations et répondent à des objectifs et modes de fonctionnement spécifiques.

4.3.1. Listes de diffusion administratives

L'objectif de ces listes est de communiquer des informations officielles aux AGENTS ou aux USAGERS de l'UPPA.

Les listes concernées sont :

- uppa-admin-securite@univ-pau.fr
- uppa-admin@univ-pau.fr

- l-etudiants@univ-pau.fr

Les règles de fonctionnement sont les suivantes :

- seuls les services habilités sont autorisés à poster des méls (pas de réponse possible des AGENTS et USAGERS)
- l'inscription est automatique et la désinscription n'est pas possible
- méls modérés par les personnels autorisés

4.3.2. Listes de diffusion inter-agents

L'objectif de ces listes est de permettre les échanges entre AGENTS de l'UPPA.

Les listes concernées sont :

- uppa-infos@univ-pau.fr
- uppa-forum@univ-pau.fr

Les règles de fonctionnement sont les suivantes :

- tous les abonnés de la liste sont autorisés à poster des méls
- l'inscription est automatique et la désinscription est possible
- pas de modération

4.3.3. Liste de diffusion inter-usagers

L'objectif de cette liste est de permettre les communications syndicales et associatives vers les USAGERS de l'UPPA.

La liste concernée est :

- infos-entre-etudiants@univ-pau.fr

Les règles de fonctionnement sont les suivantes :

- seuls les représentants d'organisations syndicales et d'associations étudiantes sont autorisés à poster des méls
- l'inscription est automatique et la désinscription est possible
- pas de modération

Dans le cadre du bon usage des listes de diffusion, la direction se réserve le droit de vérifier la conformité des échanges à la présente charte.

En cas de manquement à la présente charte, la direction se réserve le droit de suspendre le droit de diffusion aux personnes et à la structure qu'elle représente.

De façon générale, l'utilisation des listes de diffusion est soumise aux règles du chapitre « IX. Réglementation applicable et sanctions ».

4.3.4. Confidentialité des listes de diffusion administratives

Il convient de ne pas envoyer conjointement à uppa-admin (ou à uppa-admin-securite) et à la liste des étudiants. Il en va de même pour les méls et les listes extérieures à l'UPPA. Pour les diffusions internes, la bonne pratique est de dupliquer les messages par liste de diffusion ; notamment, pour la liste des étudiants qui doit être utilisée séparément.

Lors d'un envoi sur plusieurs listes de diffusion en même temps, penser à vérifier qu'elles ne sont pas redondantes.

Lors de la rédaction d'un mél ou d'une réponse, il convient de ne pas utiliser les adresses des listes uppa-admin et uppa-admin-securite car cela encombre la modération qui rejettera les messages.

4.3.5. Limitation de l'impact environnemental des listes de diffusion

Dans le cadre de l'envoi d'un mél aux listes de diffusion, il est fortement recommandé d'éviter les documents en pièce-jointe car cela génère un stockage énergivore : utiliser plutôt l'application de dépôt **https://filesender.renater.fr/**. Cette application offre l'avantage de comptabiliser les téléchargements et de pouvoir ainsi mesurer l'impact d'une diffusion.

5. ESPACES DE STOCKAGE UPPA

L'UPPA met à la disposition des AGENTS différents moyens de stockage :

- Cloud privé : https://nuage.univ-pau.fr/
- Lecteurs réseau accessibles depuis les postes de travail : par exemple le lecteur S:
- GED : gestion électronique de documents
- Stockage formation : elearn
- Stockage recherche : cluster de calcul et iRODS

Les autorisations d'accès à ces espaces sont données à chaque usager selon les besoins de sa fonction.

Chaque usager veille à maintenir un niveau de stockage cohérent avec son activité et à ne pas stocker de fichiers inutilement afin de limiter les coûts financiers et énergétiques que cette pratique engendrerait.

Dans tous les cas, il est formellement interdit de stocker des fichiers aux contenus illicites.

6. POSTE DE TRAVAIL INFORMATIQUE

L'université met à disposition de ses AGENTS et de ses USAGERS des équipements adaptés à leur profil, majoritairement des ordinateurs fixes et portables.

Ces équipements sont destinés à un usage professionnel pour les AGENTS et pédagogique pour les USAGERS. Ils sont acquis dans le cadre du règlement intérieur de l'achat public (RIAP) et mis en service par le pôle numérique de l'université.

6.1. Ordinateur en libre-service

L'ordinateur en libre-service est réservé aux activités de l'établissement. L'usager du numérique est tenu de s'authentifier avec ses propres identifiant et mot de passe. Sa connexion est soumise à la traçabilité de l'accès au poste.

Toute installation de logiciels externes et modification de la configuration ou du système est interdite sauf dans le cas d'une autorisation expresse.

Lors de l'utilisation d'un ordinateur en libre-service, l'usager s'engage à verrouiller sa session en cas d'absence temporaire.

Les ordinateurs en libre-service peuvent être réinitialisés à tout moment, aussi il est préférable qu'aucune information ne soit laissée dans la session de l'ordinateur.

Après sa séance de travail, l'usager du numérique doit fermer sa session.

6.2. Ordinateur professionnel

L'usager du numérique s'engage à protéger les équipements mis à sa disposition, pour cela il doit :

- utiliser les moyens adaptés pour garantir la sécurité des équipements mobiles et fixes (câble antivol, rangement dans un tiroir ou une armoire fermant à clé, etc.) ;
- verrouiller ou fermer sa session sur le poste de travail, en cas d'absence, même pour une courte durée ;
- signaler sans délai à l'établissement toute perte, vol ou compromission d'un équipement mis à sa disposition en ouvrant un ticket d'assistance (https://assistance.univ-pau.fr/) ;
- privilégier les espaces et périphériques de stockage fournis par l'université ;
- ne jamais connecter, à un poste de travail, un périphérique venant de l'extérieur sans l'avoir fait tester au préalable (par exemple, une clé USB trouvée par terre ou près d'un poste). Une attention particulière devra être portée aux « goodies » et autres cadeaux USB ;
- respecter les procédures de mises à jour automatique mises en place par le pôle numérique ;
- installer uniquement les logiciels autorisés explicitement par l'université ;
- s'abstenir de se connecter à des sites suspects et éviter de télécharger des logiciels à la provenance douteuse ou piratés ;
- s'assurer de toujours utiliser des logiciels dans le respect des licences libres ou commerciales dont il a préalablement pris connaissance.

En outre l'usager du numérique a l'obligation d'apporter tous les soins nécessaires à la bonne conservation du matériel qui lui est prêté et ne doit à aucun moment le laisser sans surveillance.

En cas de dysfonctionnement technique, d'intrusion ou de tentative d'attaque sur les systèmes informatiques, les administrateurs du numérique peuvent utiliser les journaux ou traces présentes sur un poste de travail pour tenter de retrouver l'origine du problème. Ces personnels sont soumis à une obligation de confidentialité. Pour cette raison, ils ne peuvent pas prendre connaissance du contenu des répertoires, fichiers ou messages explicitement désignés comme « privé » ou « personnel ».

L'usager du numérique s'engage à adopter un comportement qui ne porte pas atteinte aux droits ou à l'image de l'UPPA ou de tiers.

Si l'usager du numérique est suspecté d'avoir une utilisation non appropriée de son poste professionnel (par exemple consultation fréquente et prolongée de sites pornographiques) un audit du poste concerné peut être demandé auprès des services informatiques sous la supervision du RMSI, de la DPO et du supérieur hiérarchique.

À l'occasion de cet audit, une inspection sécurité des journaux du poste, ou de ses connexions vers Internet, sera menée par un correspondant de sécurité du numérique (CSSI) ou une société spécialisée en présence du RMSI et de la DPO.

L'usager du numérique s'engage à utiliser son poste dans le respect de la réglementation et par conséquent à préserver les informations à valeur de preuve qu'il peut contenir (il est rappelé que la destruction de preuve est punie par la loi).

6.3. Utilisation privée d'un ordinateur professionnel

Les ressources mises à disposition d'un usager du numérique sont réservées à l'exercice de son activité professionnelle. Un usage personnel est cependant toléré à condition qu'il :

- reste limité, tant dans la fréquence que dans la durée ;
- ne mette pas en danger la sécurité et le bon fonctionnement de l'ordinateur ;
- n'affecte pas l'usage professionnel ;
- reste non lucratif ;
- n'enfreigne pas la loi, les règlements et les dispositions internes.

Toute donnée stockée dans le SI de l'établissement est réputée professionnelle à l'exception des données explicitement désignées par l'usager du numérique comme ayant un caractère privé par la mention « personnel » ou « privé ».

De manière générale, le personnel du service informatique n'est pas autorisé à prendre connaissance du contenu des répertoires, fichiers ou messages explicitement désignés comme personnels ou privés.

Toutefois, en cas d'urgence avérée (par exemple suite à un problème de sécurité) et après information de l'usager du numérique, il est possible d'accéder à ces données. Cette démarche aura lieu en présence de la DPO, et du RMSI et avec une autorisation expresse d'une autorité de sécurité du numérique.

La sauvegarde régulière des données à caractère privé incombe à l'usager du numérique.

À son départ de l'Université, l'usager du numérique est responsable de la suppression des données privées qu'il aurait stockées dans le système d'information de l'établissement. À l'issue de la période de rétention légale, l'établissement pourra procéder à l'effacement des données de l'usager du numérique.

6.4. Droits d'administrateur sur un ordinateur professionnel

Conformément à la Politique de Sécurité des SI (PSSI), la gestion des privilèges des usagers du numérique sur leurs postes de travail doit suivre le principe du « moindre privilège ». Chaque usager du numérique ne doit disposer que des privilèges nécessaires à la conduite des actions relevant de sa mission. L'accès au compte « administrateur local » sur les postes de travail doit être strictement limité aux équipes en charge de l'exploitation et du support de ces postes de travail.

Certaines activités, notamment dans le domaine de la recherche, peuvent nécessiter l'utilisation d'un compte avec des droits d'administrateur. Dans ce cas, il convient d'utiliser un ordinateur virtuel (VM) ou un ordinateur dédié à l'expérimentation.

6.5. Connexion d'un matériel inconnu au réseau de l'UPPA

Aucun matériel inconnu, au sens hors du périmètre d'administration des services informatiques de l'établissement, ne doit être connecté au réseau filaire de l'UPPA.

En cas de besoin spécifique, une demande de connexion doit être formulée sur le système d'assistance. Cette demande sera évaluée sur le plan de la sécurité du numérique.

Pour les terminaux personnels ou BYOD[2] des usagers du numérique disposant d'un compte informatique, le réseau WiFi Eduroam, isolé du SI, est mis en place à l'université et présente le seul moyen autorisé de connexion à Internet.

6.6. Connexion d'un matériel de l'UPPA à l'extérieur des locaux

L'accès au réseau de l'Université et aux applications de l'extérieur est réalisé selon une procédure spécifique, garantissant la sécurité des échanges. Cette procédure s'appuie sur le VPN[3] qui donne accès aux applications du SI en fonction des droits d'accès de l'usager du numérique.

La présente charte est applicable dans le cadre du télétravail.

Chaque usager du numérique a la charge de contribuer, à son niveau, à la sécurité du numérique de l'UPPA notamment en faisant preuve d'une grande vigilance à son domicile ou lors de ses déplacements. Pour cela il est nécessaire de prendre en compte les bonnes pratiques suivantes :

- s'assurer de la protection contre le vol de son ordinateur portable en le rangeant dans un endroit sécurisé lorsqu'il n'est pas utilisé ou en utilisant un anti-vol ;
- ne pas laisser son ordinateur portable sans surveillance ou apparent dans un local non sécurisé ou un moyen de transport (voiture, train, avion, etc) ;
- ne pas laisser à disposition des supports informatiques (disque dur externe, clés USB, etc) contenant des informations confidentielles dans des lieux non sécurisés ;
- récupérer systématiquement les documents imprimés sur l'équipement d'impression (imprimante, photocopieur, etc) ;
- ne pas consulter des informations sensibles ou saisir des mots de passe dans les lieux publics où il est susceptible d'être surveillé ;
- utiliser un filtre de confidentialité sur les écrans d'ordinateurs portables ;
- protéger les données confidentielles par les logiciels de chiffrement validés par l'établissement en appliquant la procédure associée ;
- ne pas se connecter à des WIFI publics (aéroport, train, hôtel, etc).

L'usager du numérique doit s'assurer, auprès de son service informatique, que les données professionnelles de son ordinateur sont sauvegardées.

7. TERMINAL MOBILE

Le terminal mobile fourni par l'établissement est sous la responsabilité de l'usager du numérique.

Comme pour l'ordinateur, les accès au compte informatique UPPA doivent être effectués sur un terminal à jour uniquement (système d'exploitation et applications).

Attention ! Les terminaux mobiles connaissent une obsolescence rapide : il est important de s'assurer que le matériel est toujours suivi par le fabricant.

Il est recommandé de chiffrer vos terminaux pour préserver la confidentialité des données stockées.

2 Bring your own device : Amène ton propre matériel

3 Virtual Private Network : Système chiffré permettant la connexion d'un ordinateur UPPA depuis l'extérieur de l'établissement.

7.1. Données personnelles

L'utilisation du terminal mobile professionnel pour le stockage de données personnelles est tolérée.

Ces données sont sous la responsabilité exclusive de l'usager du numérique.

7.2. Code PIN (carte SIM)

Définir et activer un code PIN personnalisé pour qu'il soit demandé à chaque démarrage.

Ce code contrôle la carte SIM et permet de verrouiller le terminal au bout de 3 codes erronés consécutifs. Pour protéger votre terminal ne désactivez pas le code PIN et changez celui proposé par défaut.

Il est conseillé de choisir un code sans lien avec votre code de carte bancaire, date de naissance, numéro de téléphone, ou qui ne soit pas une suite logique (1234, 2468, 0000…).

7.3. Verrouillage du terminal

Il est recommandé de sécuriser son terminal mobile via un code afin de se prémunir contre l'exposition des données en cas de vol, perte ou actes malveillants. Ce code sera demandé après chaque mise en veille ou après un certain laps de temps d'inactivité.

Sur la plupart des terminaux, vous pouvez définir le délai avant mise en veille et verrouillage automatique.

7.4. Code IMEI et PUK

Le code IMEI est le numéro de série de votre terminal, il est composé de 15 à 17 chiffres. En cas de perte ou de vol, ce code sert à bloquer l'usage du terminal sur tous les réseaux mobiles. Il est indiqué sur la boite d'emballage du téléphone. Notez ce numéro et gardez-le en lieu sûr, par exemple dans votre coffre-fort électronique.

Le code PUK est lié à la carte SIM. Il permet le déverrouillage de celle-ci en cas 3 codes PIN erronés. Il est disponible dans l'emballage de la carte SIM. Conserver les codes IMEI et PUK en cas de perte ou de vol.

8. ORGANISATION DES MOUVEMENTS DES AGENTS ET DES USAGERS DE L'ÉTABLISSEMENT

Dans la présente partie, le terme « AGENT » doit être entendu comme tous types de personnel de l'UPPA et le terme « USAGERS » doit être entendu comme les usagers du service public de l'établissement notamment les étudiants.

8.1. Arrivée dans l'établissement

À son arrivée dans l'établissement, chaque AGENT se voit mettre à disposition un ordinateur, un compte informatique ainsi qu'un accès à une messagerie électronique. L'AGENT doit prendre connaissance des politiques et chartes en vigueur dans l'établissement relatives à la sécurité du numérique et à la protection des données à caractère personnel.

Il en va de même pour les ordinateurs pouvant être prêtés aux USAGERS.

8.2. En cas d'absence ou de départ de l'établissement

En cas d'absence ou de départ de l'établissement et afin de répondre à l'obligation de loyauté imposée à l'usager du numérique, ce dernier est tenu de communiquer, à son supérieur hiérarchique, les données et informations nécessaires à la poursuite de l'activité de l'Université. Le compte informatique

Le compte informatique étant l'élément essentiel d'accès au SI, il fait l'objet d'une attention particulière et notamment en cas d'absence ou de départ.

En cas d'absence ou de départ de l'établissement et afin de répondre à l'obligation de loyauté imposée à l'AGENT, ce dernier est tenu de communiquer, à son supérieur hiérarchique, les données et informations nécessaires à la poursuite de l'activité de l'Université.

Les USAGERS sont responsables de la récupération de leurs données avant la fermeture du compte informatique.

Le mot de passe doit rester confidentiel et ne doit pas être divulgué sous aucun prétexte, même à son supérieur hiérarchique.

Au départ de l'établissement, l'AGENT ou l'USAGER recevra une notification lui proposant de conserver l'accès à son compte informatique. Sans demande de sa part dans un délai d'un mois, le compte sera automatiquement fermé.

En cas de conservation du compte informatique, une notification lui sera adressée tous les ans et il devra formuler une nouvelle demande de prolongation.

Deux cas de figure peuvent se présenter : l'Usager souhaite prolonger son compte (cas de révision des droits d'accès) ou l'Usager souhaite fermer son compte.

L'AGENT ou l'USAGER s'engage à porter à la connaissance de ses interlocuteurs habituels son absence ou son départ de l'Université, par tout moyen approprié. Il lui appartient, lors de son départ définitif de l'établissement, de récupérer et d'effacer toutes données privées.

Lors du départ, le compte informatique de l'AGENT ou de l'USAGER perd les droits d'accès au SI qu'il détenait dans le cadre de ses fonctions ou de sa formation.

L'autorité d'enregistrement est habilitée à gérer les demandes de prolongation.

En cas d'absence ou de départ de l'établissement, à l'instar du compte informatique, il appartient à l'AGENT ou à l'USAGER de récupérer et d'effacer toute donnée privée. En ce qui concerne les données professionnelles contenues dans la messagerie électronique, se référer au point VIII.2.4.

8.2.1. Le matériel informatique

À son départ, l'AGENT ou l'USAGER s'engage à restituer tous les matériels informatiques mis à disposition dans le cadre de ses fonctions ou de sa formation.

8.2.2. Sort des données professionnelles

Nonobstant les dispositions de la présente charte, en cas d'impossibilité ou de refus de la part de l'AGENT ou de ses ayants-droits, l'établissement peut prendre les mesures nécessaires pour accéder aux données professionnelles contenues sur les ressources informatiques et/ou services internet de l'intéressé. Ces opérations ne peuvent s'opérer que sur demande du supérieur hiérarchique et après accord du Président de l'Université.
Selon le statut de l'AGENT et la nature des données, des dispositions particulières peuvent être prises dans le respect des dispositions en vigueur.

8.2.3. Sort des données privées

À son départ de l'Université, l'AGENT ou l'USAGER est responsable de la suppression des données privées qu'il aurait stockées dans le système d'information de l'établissement. L'établissement procédera à l'effacement des données un an après la fermeture du compte informatique.

9. RÉGLEMENTATION APPLICABLE ET SANCTIONS

9.1. Respect du règlement sur la protection des données à caractère personnel et la loi informatique et libertés

L'usager du numérique est informé de la nécessité de respecter les dispositions légales en matière de traitement automatisé de données à caractère personnel, conformément à la loi n° 78-17 du 6 janvier 1978 dite « Informatique et Libertés » modifiée par la loi du 7 octobre 2016. L'usager du numérique est informé de la nécessité de respecter la réglementation en matière de traitements (automatisés ou non) de données à caractère personnel, conformément au Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD) et à la loi n° 78-17 du 6 janvier 1978 dite « Informatique et Libertés » modifiée.

Une donnée à caractère personnel est toute information relative à une personne physique susceptible d'être identifiée directement ou indirectement.

Tout traitement impliquant des données à caractère personnel doit être conforme aux dispositions du RGPD et de la loi n°78-17 du 6 janvier 1978 dite « informatique et libertés » modifiée. Sont notamment considérés comme des traitements, les opérations suivantes : l'enregistrement, la conservation, la diffusion de données à caractère personnel sur support numérique ou papier. Sont également soumis à la réglementation les systèmes de vidéosurveillance.

En conséquence, tout usager souhaitant procéder à un tel traitement devra en informer préalablement le délégué à la protection des données (DPO) qui prendra les mesures nécessaires au respect des dispositions légales.

Par ailleurs, conformément aux dispositions de la réglementation, chaque usager du numérique dispose d'un droit d'accès, de rectification et d'opposition relatif à l'ensemble des données le concernant, y compris les données portant sur l'utilisation des systèmes d'information. Selon les cas l'usager du numérique dispose également d'un droit à la limitation du traitement et à la portabilité de ses données.

Ces droits s'exercent auprès du responsable du traitement en faisant copie au délégué à la protection des données (DPO) de l'établissement : dpo@univ-pau.fr

Pour plus d'informations, il convient de consulter les politiques de l'établissement en matière de protection des données à caractère personnel. Elles sont disponibles sur la page d'accueil du site de l'établissement https://www.univ-pau.fr/ dans la rubrique Recueil des Actes Administratifs.

9.2. Cas de la journalisation

Conformément au RGPD et à la recommandation de la CNIL, l'établissement est dans l'obligation légale de mettre en place un système de journalisation des accès internet, de la messagerie et des données échangées. Afin d'en assurer la traçabilité, toutes les activités numériques sur les postes, sur les serveurs et sur Internet génèrent **des enregistrements qui sont conservés pendant un an**.

Ces enregistrements sont indispensables pour la sécurité des données à caractère personnel. Ils peuvent notamment permettre de détecter des incidents de sécurité ou des accès non autorisés. Dans ce cas, seuls les administrateurs du numérique désignés par l'autorité d'homologation peuvent exploiter ces enregistrements.

9.3. Respect de la propriété intellectuelle

En application des dispositions du Code de la propriété intellectuelle (notamment les articles L.111-1 et L.112-2, article L.335-3) relatives à la propriété littéraire et artistique, toute copie d'informations protégées (logiciels, images, textes, musiques, sons, etc.) est illicite. De même, toute reproduction, tout téléchargement, copie, modification, utilisation ou diffusion de logiciels, bases de données, pages web, images, photographies ou autres créations protégées doit se faire conformément au droit d'auteur.

9.4. Limites de la liberté d'expression

En application de la loi du 29 juillet 1881 sur la liberté de la presse et divers textes publiés depuis cette date réglementent la liberté d'expression, il est interdit de diffuser des informations constituant des atteintes à la personne (injure, discrimination, racisme, xénophobie, antisémitisme, révisionnisme, complotisme, diffamation, obscénité, harcèlement ou menace) ou pouvant constituer une incitation à la haine, à la violence ou une atteinte à l'image d'une autre personne.

9.5. Pédopornographie

La consultation ou la détention d'images pédopornographiques est sévèrement réprimée par les articles L.227-23 et suivants du Code pénal. L'établissement assumera son devoir de signalement au Procureur de la République (article 40 du Code de procédure pénale) de tout usager du numérique détenant ou consultant de telles images.

9.6. Atteinte aux systèmes de traitement automatisés des données (STAD)

Conformément à la réglementation relative aux atteintes aux systèmes de traitement automatisé de données prévue par les articles 323-1 à 323-7 du Code pénal, il est interdit d'accéder ou de se maintenir dans un réseau informatique frauduleusement, d'entraver le fonctionnement d'un système ou de modifier frauduleusement des données. L'usager du numérique se doit de respecter les privilèges et droits d'accès qui lui sont attribués.

9.7. Limitations et sanctions applicables en cas de non-respect des règles définies

Le non-respect des règles établies par la présente charte pourra donner lieu à une suspension, à titre conservatoire, de l'accès aux ressources numériques sur décision du Président.

De plus, ce non-respect pourra également donner lieu à une saisine de la section disciplinaire du conseil académique de l'établissement conformément à la réglementation en vigueur, indépendamment d'éventuelles sanctions civiles ou pénales.

10. ENGAGEMENTS

10.1. Engagement individuel de tout usager des ressources numériques de l'UPPA

Chaque AGENT et USAGERS de l'établissement est tenu de lire et d'accepter la « Charte des usagers du numérique » dans l'application de gestion des comptes informatiques **https://moncompte.univ-pau.fr/**.

10.2. Engagement individuel de responsabilité de l'usager du numérique en tant qu'administrateur de son poste de travail

Les postes de travail utilisés par les AGENTS sont configurés et administrés par les services numériques de l'établissement. Ils répondent aux critères de sécurité définis dans la PSSI qui interdit notamment à l'usager du numérique de disposer des droits d'administration de son poste.
Les droits d'administration peuvent être consentis exceptionnellement et temporairement sur demande justifiée de l'usager du numérique. Il devra donc faire l'objet d'un renouvellement à échéance.
Disposer de ce droit engage la responsabilité de l'usager du numérique sur le maintien en conditions opérationnelles et de sécurité de son poste de travail. C'est-à-dire qu'il devient responsable de la gestion des mises à jour, de la surveillance des alertes émises par les dispositifs de sécurité et du bon fonctionnement général du poste.
En cas d'altération par l'usager du bon fonctionnement du poste de travail ou d'atteinte à sa sécurité, les droits d'administration pourront être révoqués et le poste remis en conformité.
Voir les modalités détaillées en annexe.

11. ANNEXES

11.1. Demande de droits d'administration d'un poste de travail

De manière exceptionnelle, certains usagers du numérique peuvent avoir besoin des droits d'administration de leur poste. La procédure d'attribution d'un compte administrateur local est dérogatoire : elle est motivée par une situation bien identifiée.
En préalable, avec l'aide des informaticiens du CSP Numérique Proximité, tout doit être fait pour envisager d'autres possibilités, et les droits d'administration du poste ne doivent être attribués qu'en dernier recours, quand aucune autre solution n'a été trouvée.
Ensuite l'accord du supérieur hiérarchique est indispensable.

Cette possibilité est offerte sur justification et après validation du CSP Numérique Proximité et du RMSI.
Dans ce cas, l'usager du numérique souhaitant disposer des droits d'administration en fait la demande par ticket d'assistance, et s'engage à respecter les bonnes pratiques de co-administration.

Cadre d'utilisation du compte administrateur local

- les usagers du numérique ne doivent pas se connecter avec le compte administrateur local, mais utiliser temporairement le mécanisme d'élévation de privilèges à partir de leur compte standard ;

- un compte d'administration local, différent du compte standard, permet d'installer des applications et des périphériques supplémentaires. Ce compte autorise également la modification de la configuration du poste de travail.

Obligations de l'usager du numérique administrateur de son poste de travail

- veiller à la confidentialité du mot de passe du compte d'administration ;
- ne pas créer de compte pour d'autres usagers du numérique sur son poste ;
- ne jamais travailler sous le compte d'administrateur local et agir avec précaution ;
- conserver, sans les modifier, les mécanismes de sécurité qui sont mis en place par le pôle numérique (par exemple : mises à jour automatiques, anti-virus, logiciel d'inventaire, système d'authentification et de gestion centralisée des équipements, etc) ;
- accepter les futures révisions des mécanismes de sécurité ;
- conserver, sans les modifier, les autres comptes locaux existants (root, administrateur, etc) ;
- s'assurer de la provenance et de l'intégrité des logiciels qu'il installe lui-même (absence de logiciels espions ou malveillants).

En cas de dysfonctionnement ou de panne logicielle bloquant le poste de travail

- l'intervention du pôle numérique se limitera à une réinstallation dans l'état initial ;
- la sauvegarde/restauration des données stockées localement sur le poste de travail et la réinstallation des logiciels non gérés par le pôle numérique restent à la charge de l'usager du numérique.

Les usagers du numérique choisissant de disposer de droits administrateurs sur leur poste s'engagent à respecter l'ensemble des lois, règlements, chartes et politiques en vigueur dans l'établissement.
En cas de non-respect de ces règles, la direction du numérique est autorisée à retirer l'accès au réseau de l'établissement afin de ne pas mettre en danger le système d'information.