Université de Strasbourg

CHARTE DE BON USAGE DES MOYENS NUMÉRIQUES DE L'UNIVERSITÉ

Guide de l'utilisateur

Frédéric DEHAN
Directeur général des services

Affaire suivie par
Guy BRAND
Responsable de la sécurité
des systèmes d'information
Tél. : +33 (0)3 68 85 06 88
gb@unistra.fr

SOMMAIRE

Préambule

Le présent guide pratique de l'utilisateur a pour objet d'accompagner les personnes autorisées à accéder au système d'information de l'Université de Strasbourg dans la mise en œuvre des règles de sécurité et de comportement préconisées par la charte de bon usage des moyens numériques.

Avec la charte, le présent guide complète le règlement intérieur régissant l'usage des moyens numériques que l'Université de Strasbourg met à disposition de ses utilisateurs.

Les utilisateurs sont informés que la violation des prescriptions du présent guide peut entraîner des sanctions. La nature des sanctions encourues est précisée dans l'annexe juridique de la charte.

La charte et les documents qui la complètent, tels l'annexe juridique et le présent guide de l'utilisateur, peuvent être consultés dans l'environnement numérique et social de travail de l'Université de Strasbourg, dénommé Ernest.

Rappels :

- Que sont les « moyens numériques » ?

Les moyens numériques de l'Université de Strasbourg sont définis, par l'article I. al. 2 de la charte des bons usages, comme « *l'ensemble des logiciels et matériels, outils informatiques et services numériques, que l'Université de Strasbourg met à disposition de ses utilisateurs* ».

- Qui sont les « utilisateurs » ?

La notion d'« utilisateurs » est définie à l'article I. al. 3 de la charte comme « *l'ensemble des personnes ayant obtenu l'autorisation d'accéder au système d'information de l'Université de Strasbourg* ».

I. Règles de Sécurité

Gestion des mots de passe

Chaque utilisateur doit veiller au respect de la sécurité liée aux mots de passe permettant l'accès à son environnement de travail (logiciels métiers, Ernest, ...).

Un bon mot de passe est long, constitué de 8 caractères alphanumériques au minimum - 12 sont fortement recommandés. Il doit être unique et différent pour chaque compte. Chaque utilisateur est personnellement responsable des mots de passe qu'il a choisis.
Concrètement, chaque utilisateur doit :

- choisir un mot de passe robuste et n'ayant aucun lien avec son environnement familier ;
- veiller à la confidentialité de son mot de passe et notamment s'abstenir de l'écrire sur un support facilement accessible ;
- changer immédiatement son mot de passe en cas de doute sur sa confidentialité.

Paramétrage des postes de travail

a) Principes généraux

Le poste de travail de l'utilisateur constitue un outil qui doit être protégé des intrusions. À cet égard il est conseillé, à chaque fois que cela sera possible :

- de paramétrer la mise en veille automatique de l'ordinateur avec demande du mot de passe pour sa réactivation après une période d'inactivité ;
- d'effectuer systématiquement une déconnexion des serveurs réseaux et de clore les applications actives avant de quitter son poste de travail.

b) Protections logicielles : anti-virus et pare-feu (« firewall »)

Un anti-virus est un logiciel de protection dont le but est de détecter les virus ou logiciels malveillants (comme les « vers » ou les « chevaux de Troie »). Pour cela, il inspecte la mémoire, les disques durs de l'ordinateur et les volumes amovibles (CD, DVD, clé USB, disque dur externe…) pour vérifier que les fichiers présents ne contiennent pas de codes malveillants connus. Il permet aussi d'effectuer régulièrement des analyses planifiées.

Un anti-virus protège contre les codes malveillants qu'il connaît ou qu'il reconnaît. Il est donc non seulement indispensable d'utiliser un anti-virus, mais aussi de veiller à sa mise à jour.

Un pare-feu ou « firewall » permet de protéger l'ordinateur connecté à Internet des attaques externes initiées par des programmes ou des personnes malveillants.

Ces mesures de protection sont mises en place par la Direction du numérique sur les postes informatiques qu'elle gère ; elles sont à la charge de l'utilisateur pour les équipements dont il est administrateur.

c) Mises à jour

Les logiciels, comme toute création humaine, comportent des défauts. Parmi ces défauts, on en trouve qui portent atteinte à la sécurité ; ils sont appelés « vulnérabilités ». Au quotidien, de nombreuses vulnérabilités sont découvertes dans les systèmes d'exploitation et les logiciels équipant les matériels informatiques. Ces failles sont très rapidement exploitées par les pirates les plus expérimentés pour tenter de prendre le contrôle ou de voler des informations sur les postes de travail et les serveurs.

Il est donc primordial d'appliquer systématiquement les mises à jour de sécurité, au fur et à mesure de leur publication. Cette maintenance est assurée par la Direction du numérique sur les postes informatiques qu'elle gère ; elle est à la charge de l'utilisateur pour les équipements dont il est administrateur.

d) Les accessoires du poste de travail, dont les périphériques de stockage

Les périphériques et particulièrement les périphériques de stockage comme les clés USB, les disques durs externes, les cartes mémoire - voire les téléphones portables ou baladeurs qui offrent cette fonctionnalité - sont un vecteur de plus en plus utilisé pour infecter les postes de travail.
Un périphérique de stockage d'origine inconnue peut non seulement contenir des virus, mais également être configuré pour « aspirer » le contenu du poste de travail à l'insu de l'utilisateur.

Il est donc vivement déconseillé d'utiliser un matériel d'origine inconnue, particulièrement pour un échange de données.
D'une manière générale, il est recommandé de séparer les usages entre les périphériques de stockage professionnels et privés.
Les membres du personnel de l'Université de Strasbourg autorisés à exercer leurs missions en télétravail veilleront à appliquer cette recommandation avec une particulière vigilance, conformément aux exigences des articles 4.11 de la charte du télétravail, 2.5 et 2.6 du protocole individuel.

e) Utilisation du poste en mode administrateur

Un compte ayant les droits « administrateur » offre à son titulaire un contrôle très étendu sur les logiciels équipant le poste informatique. Les comptes administrateurs sont ainsi les cibles privilégiées de nombreux programmes malveillants tentant d'accéder aux ressources du poste.

Il est vivement recommandé d'utiliser au quotidien - et en particulier pour naviguer sur internet - un compte ne possédant pas les privilèges « administrateur ».

D'une manière générale, l'attention des personnels disposant de ces privilèges sur un poste informatique est attirée sur leur responsabilité dans la gestion des mises à jour et la surveillance des alertes émises par les dispositifs de protection antivirale.

Messagerie électronique

L'attention des utilisateurs est attirée sur les facteurs de risques liés aux mésusages de la messagerie électronique :

- son coût environnemental, lié au volume - nombre et poids - des messages transmis,
- son impact sur la qualité de vie au travail,
- les menaces pour la confidentialité des données et la sécurité informatique.

Une utilisation raisonnée de la messagerie s'impose pour répondre à ces enjeux : un ensemble de bonnes pratiques est exposé dans la Charte sur la qualité de vie au travail, dont la nécessité de restreindre l'usage de la messagerie électronique aux échanges professionnels, de limiter l'envoi des pièces jointes et de circonscrire au strict nécessaire le nombre de destinataires d'un message.

a) Rappel concernant les messages à caractère privé

Aux termes de la charte de bon usage des moyens numériques (Art.II, Section II.1), le terme « professionnel » vise les usages n'ayant pas un caractère strictement privé. Le caractère privé n'est reconnu qu'aux actes détachés de l'exercice des missions confiées (pour les enseignants-chercheurs, les enseignants et le personnel administratif, technique de l'Université de Strasbourg) ou détachés des activités pédagogiques (pour les utilisateurs étudiants).

Tout message à caractère strictement privé, reçu ou émis, doit comporter en objet la mention « Privé », afin d'exprimer sans ambiguïté le caractère extra-professionnel du message.

Les messages ne comportant pas, en objet, cette mention sont réputés professionnels.

b) Caractéristiques et limitations de la messagerie électronique

L'envoi de messages contenant des pièces jointes est une pratique énergivore, coûteuse en termes de ressources et potentiellement dangereuse pour le poste de travail. Les utilisateurs veilleront à ne l'utiliser qu'en cas de nécessité, en privilégiant pour leurs usages courants les outils collaboratifs et de partage sécurisé proposés par l'Université de Strasbourg, dont l'outil de stockage en ligne Seafile.
Pour prévenir les abus, les messages émis ou reçus font l'objet d'une limitation technique de leur taille.

En cas de dépassement de la taille limite, le message est rejeté et l'émetteur reçoit un message de non distribution.

Par ailleurs, l'envoi de messages à un grand nombre de destinataires doit être proscrit.
Cette pratique provoque le ralentissement des serveurs de messagerie de l'établissement.
Surtout, les prestataires externes de services de messagerie assimilent ces messages à des pourriels ou « spams » et, en conséquence, placent l'université sur une liste noire. Ceci entraine le blocage, chez ces prestataires, de tous les messages en provenance de l'université.

Pour prévenir de tels dysfonctionnements, une limite technique est mise en œuvre par la direction du numérique : en cas d'abus, le compte de l'expéditeur est bloqué.
S'il est nécessaire de diffuser des messages à de très nombreux destinataires, il est impératif d'utiliser les listes de diffusion (et notamment le service Sympa), qui ne provoquent aucune perturbation.

c) Stockage et archivage des messages électroniques

L'utilisateur doit mettre en œuvre les moyens nécessaires à la conservation des messages qui pourraient être indispensables à son activité.

La messagerie des personnels de l'Université de Strasbourg est sauvegardée quotidiennement, ce qui ne dispense en aucun cas les utilisateurs de procéder à un archivage personnel. En procédant ainsi, les usagers peuvent plus facilement purger leurs boîtes de messagerie et, par conséquent, réduire l'impact de leur correspondance électronique sur les serveurs de l'université, aussi bien en termes de stockage que de

consommation électrique.

Chaque utilisateur doit en conséquence organiser lui-même la conservation de ces éléments en décidant :

- du nombre de sauvegardes et de leur périodicité ;
- du choix des fichiers et messages conservés et de ceux qui sont détruits ;
- de la méthode et de la durée de stockage.

d) Sécurité antivirale

De manière générale, il est déconseillé d'ouvrir des fichiers en provenance d'un expéditeur inconnu. Cette prescription concerne en particulier les fichiers compressés ou exécutables dont l'ouverture peut notamment générer l'activation de virus informatiques, de codes malveillants, susceptibles d'entraîner des conséquences d'une extrême gravité pour l'Université de Strasbourg.

Les utilisateurs sont informés que l'Université de Strasbourg se réserve le droit de retenir, d'isoler et / ou de supprimer tout message à l'aide de moyens automatisés et ce, sans que ces messages aient été nécessairement ouverts, afin de s'assurer de leur innocuité.

Les utilisateurs sont informés que tout message bloquant ou présentant une difficulté technique d'acheminement à son destinataire peut être détruit sur décision de la Direction du numérique.

Les administrateurs du système d'information sont autorisés, en cas de difficultés majeures, à arrêter les services réseaux.

Navigation sur Internet (Web)

Il est rappelé que l'accès à Internet n'est autorisé qu'au travers des dispositifs de sécurité mis en place par l'Université de Strasbourg.

Certains sites malveillants profitent des failles des navigateurs pour récupérer les données présentes sur le poste de travail. D'autres sites mettent à disposition des logiciels qui, sous une apparence anodine, peuvent prendre le contrôle de l'ordinateur et transmettre son contenu à des tiers, à l'insu de son utilisateur.
La prudence est recommandée avant tout téléchargement, particulièrement pour les utilisateurs qui disposent des privilèges d'administrateur de leur poste. Les utilisateurs doivent s'abstenir de se connecter à des sites suspects et éviter de télécharger des logiciels dont l'innocuité n'est pas garantie ; par exemple : vérifier la pérennité du logiciel et / ou la nature de l'éditeur.

Sauvegarde de données : quelques repères

La sauvegarde doit être organisée sur tout type d'appareil utilisé à titre professionnel, du poste informatique fixe au matériel nomade

La Direction du numérique organise une sauvegarde des données sur un ensemble de postes informatiques qu'elle gère.

Pour tous les autres, une sauvegarde régulière par chaque utilisateur est l'unique moyen de garantir la pérennité des données et de se prémunir contre les conséquences néfastes d'un problème technique, d'une attaque informatique ou d'un vol.

Matériel nomade

a) Principes généraux

Lorsqu'un équipement nomade, de type appareil photo numérique, caméscope, téléphone mobile, ordinateur portable ou tablette, est confié à un utilisateur de l'Université de Strasbourg, cette mise à disposition :

- est réputée intervenir dans le cadre exclusif des activités professionnelles du bénéficiaire ;
- entraine l'obligation pour le bénéficiaire d'apporter tous les soins nécessaires à la bonne conservation de ce matériel.

Par exemple, le bénéficiaire doit veiller particulièrement à :

- ne pas altérer sa configuration logicielle
- ne pas exposer l'équipement confié à la chaleur ni à l'humidité ;
- ne pas le laisser sans surveillance ;
- ranger le matériel non-utilisé dans un endroit sécurisé.

Pour des raisons de sécurité, l'accès au réseau filaire des bâtiments de l'établissement est réservé au matériel confié par l'Université de Strasbourg, aucun autre matériel ne doit y être connecté.

b) Vol / Perte

En cas de vol de l'équipement confié, une déclaration doit être effectuée sans délai au commissariat de police le plus proche. Une copie de cette déclaration devra être adressée à l'Université de Strasbourg par l'intermédiaire du support informatique dont les coordonnées sont rappelées plus bas.

Toute fausse déclaration est passible de sanctions disciplinaires et / ou de poursuites pénales.

En cas de perte de l'équipement confié, une déclaration détaillée doit être adressée à l'Université de Strasbourg par l'intermédiaire du support informatique dont les coordonnées sont rappelées plus bas.

c) Détérioration

En cas de détérioration du matériel nomade prêté, celui-ci doit être restitué au responsable de l'Université de Strasbourg qui a autorisé le prêt, avec un descriptif des dommages constatés et un exposé des circonstances à l'origine de la détérioration.

Absences, départs ou mutations

Aux termes de l'article II.2 de la charte de bon usage des moyens numériques, il appartient à tout membre du personnel, quittant à titre provisoire ou définitif l'Université de Strasbourg, de respecter deux obligations :

- permettre l'accès à ses données professionnelles en vue de garantir la continuité de service ;
- procéder à la suppression des données privées qu'il aurait stockées dans le système d'information.

a) Suppression des données privées

L'attention des agents et des enseignants de l'Université de Strasbourg est attirée sur la nécessité de prendre en charge personnellement la récupération puis la suppression des données privées qu'ils auraient stockées dans le système d'information de l'établissement.
En conséquence, l'Université de Strasbourg ne peut être tenue responsable :

- de la perte des données qui n'auraient pas été récupérées par l'utilisateur avant son départ,
- de la divulgation ultérieure de données qu'il n'aurait pas supprimées.

b) Préparer son absence

Au-delà de la suppression des données privées, il incombe également au supérieur hiérarchique de l'agent qui s'apprête à quitter l'établissement de :

- demander la suppression des accès aux logiciels, applications de travail (SIFAC, SOSIE, …) ;
- faire retirer l'adresse électronique professionnelle des différentes listes de diffusion ;
- s'assurer que l'agent en question aura mis en place un « répondeur » sur sa messagerie électronique, afin d'orienter les demandeurs vers un autre contact, au plus tard le jour de son départ effectif.

II. Besoin d'aide ?

Assistance

En cas de besoin d'assistance ou de renseignements complémentaires, vous pouvez adresser vos demandes au support informatique de l'université, du lundi au vendredi, de 7H45 à 18H00 :

- par le formulaire en ligne : http://support.unistra.fr
- par courrier électronique : support@unistra.fr
- par téléphone : 03 68 85 43 21 (ou 54321 depuis un poste interne)

Données à caractère personnel

Le contact privilégié pour l'exercice des droits reconnus par la règlementation « Informatique et Libertés » et pour toutes questions relatives à la protection des données à caractère personnel, est le délégué à la protection des données de l'Université de Strasbourg : dpo@unistra.fr

Mise à jour et disponibilité des documents de référence

L'environnement numérique et social de travail Ernest recense les documents de référence mis à la disposition des utilisateurs de l'Université de Strasbourg.

La charte de bon usage des moyens numériques et l'intégralité de ses annexes – dont le présent guide pratique - sont consultables, dans leur dernière version, via Ernest.

LE PRÉSENT GUIDE PRATIQUE FERA L'OBJET DE MISES À JOUR ET IL APPARTIENT À L'UTILISATEUR DE PRENDRE CONNAISSANCE DE TOUTE NOUVELLE VERSION QUI SERA PUBLIÉE, À L'ADRESSE : https://ernest.unistra.fr