L'académie de Strasbourg

CHARTE INFORMATIQUE D'USAGE DES OUTILS NUMERIQUES PERSONNEL DES SERVICES ACADEMIQUES

Guide des bonnes pratiques

Version 1.0 Février 2015

Document principal
Document de synthèse
Annexe juridique

Rectorat de l'académie de Strasbourg
6 Rue de la Toussaint
67975 Strasbourg cedex 9

académie Strasbourg
MINISTÈRE DE L'ÉDUCATION NATIONALE, DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE

Sommaire

Préambule

Le présent guide des bonnes pratiques a pour objet d'accompagner les utilisateurs dans l'usage des outils technologiques au sein de l'académie de Strasbourg.

En complément de la charte, le présent guide expose les pratiques et le comportement que l'utilisateur doit adopter afin de respecter les exigences de sécurité informatique préconisées par l'académie de Strasbourg.

Tout signataire de la charte, est dans l'obligation de respecter les bonnes pratiques. La violation de ces obligations peut entrainer des sanctions disciplinaires, voir pénales (voir annexe juridique de la charte).

Pour rappel, la charte s'applique à l'ensemble du personnel académique, tout statut confondu, titulaires, contractuels et stagiaires. Elle s'applique également aux personnes externes aux services académiques ayant recours, même ponctuellement, aux outils informatiques de l'académie de Strasbourg.

La charte définit comme étant un **utilisateur** « *toute personne ayant accès, dans le cadre de l'exercice de son activité professionnelle, aux ressources du système d'information quel que soit son statut*.».

Elle considère comme étant des **outils numériques** l'ensemble du matériel, logiciel, outils informatiques et services numériques mis à la disposition de l'utilisateur par l'académie de Strasbourg.

Article I – Poste de travail

Par définition, **un poste de travail** est considéré comme étant l'ensemble des moyens techniques (écran, ordinateur, imprimante, portable, téléphone …) mis à la disposition de l'utilisateur. Ce matériel nécessite une utilisation vigilante et raisonnable dans le cadre des missions professionnelles de l'utilisateur.

Section 1.1 La sécurisation du poste de travail

Pour optimiser la sécurité du poste :

1- il est obligatoire pour chaque utilisateur de sécuriser son poste de travail par un mot de passe fort et non communiqué, devant être renouvelé régulièrement.

2- lorsque l'usager décide d'utiliser des supports amovibles tels que des clés USB, ce dernier doit soumettre le support à une analyse de l'antivirus.

3- lorsque l'utilisateur quitte momentanément son poste, ce dernier **doit verrouiller son poste** (Ctrl+Alt+Suppr ou touche Windows+L) ainsi que configurer et activer l'écran de veille avec protection par mot de passe. En fin de journée, il est conseillé à tout utilisateur **d'arrêter son poste de travail**.

4- les ordinateurs portables mis à disposition des personnels seront protégés au moyen d'un logiciel de chiffrement préconisé par l'académie. L'objectif est que les données stockées sur ces matériels ne soient accessibles que par le détenteur du mot de passe spécifique.

Section 1.2
Le compte de l'utilisateur

L'utilisateur possède un compte d'identification pour accéder au contenu de son poste et aux applications personnelles. Cet **identifiant** et ce **mot de passe** sont strictement **personnels** et **confidentiels**. L'utilisateur est responsable de leur conservation et s'engage à ne pas les divulguer et à ne pas s'approprier ceux d'un autre utilisateur.

Le mot de passe attribué par défaut doit être modifié.

Pour changer le mot de passe de la messagerie, rendez-vous sur le webmail.

Section 1.3
La protection logicielle : anti-virus et pare-feu (« firewall »)

Un **anti-virus** est un logiciel de protection qui permet d'identifier, neutraliser et éliminer les intrusions de logiciels malveillants tel que les virus informatiques.
L'anti-virus analyse la mémoire, les disques durs, le matériel amovibles (clé USB, CD …), le courrier électronique et la mémoire.

Il est obligatoire pour chaque poste de travail au sein de l'académie, de disposer de l'anti-virus académique. Il est interdit de désactiver cet anti-virus ou d'installer un autre outil que celui supporté par l'académie.

Un **pare-feu** ou firewall permet de protéger l'ordinateur des tentatives d'attaques effectuées par le réseau local ou internet. Il est interdit de désactiver le pare-feu ou d'installer un autre outil que celui supporté par l'académie.

Section 1.4
La sauvegarde des données

L'académie de Strasbourg met à disposition des utilisateurs :

- Des espaces de stockage de documents professionnels communs à notre service et à l'académie.
- Un espace de stockage de documents professionnels propre à chaque utilisateur.

Ces lecteurs servent uniquement à stocker des documents de travail. Tout stockage de documents privés est interdit sur ces supports.

Pour des raisons de maintenance de l'espace disque, les équipes techniques se réservent le droit d'analyser l'espace pris par l'utilisateur et le cas échéant d'optimiser l'espace qu'il occupe.

Il est vivement recommandé de faire régulièrement des sauvegardes sur ce lecteur afin d'éviter toute perte de données et de ne conserver que les fichiers ayant un intérêt pour l'activité professionnelle.

Les supports amovibles en particulier les clés USB ne doivent pas être utilisés comme un moyen de stockage principal (risque de perte/vol important).

Section 1.5
L'utilisation du poste en mode administrateur

L'utilisation d'un compte avec des droits « administrateur » offre des droits étendus à l'utilisateur. En effet l'administrateur dispose d'un accès total à l'ordinateur et peut effectuer toutes les modifications souhaitées. Ce mode de paramétrage ouvre la brèche à de nombreux programmes malveillants tentant d'accéder aux ressources du poste de

travail. La configuration en mode « administrateur » sera limitée et devra être motivée par le chef de services.

Afin d'éviter toute contamination, les postes sont configurés en mode « standard ». Ce mode d'utilisation permet aux utilisateurs d'utiliser la plupart des logiciels.

Section 1.6 L'utilisation du matériel nomade

L'académie de Strasbourg met à disposition de certains utilisateurs des ordinateurs portables, téléphones portables, tablettes … .

Ces outils sont réputés n'être utilisés que dans le cadre professionnel et uniquement par son bénéficiaire. Ledit bénéficiaire est seul responsable du matériel, de ce fait il doit veiller à son entretien courant et à sa bonne conservation.

En cas de détérioration, de perte ou de vol de ce matériel, l'utilisateur est tenu d'en informer son responsable hiérarchique dans les plus brefs délais.

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

Section 1.7 L'utilisation d'outils personnels

La connexion d'ordinateurs portables personnels au réseau interne de l'académie de Strasbourg n'est pas autorisée.

Seul le matériel fourni par l'académie est autorisé à se connecter au réseau de l'académie de Strasbourg.

Section 1.8 Le téléchargement

L'utilisateur s'engage à ne pas installer de logiciels sans y être autorisé. Tout téléchargement de logiciel doit se faire avec vigilance et dans le respect du droit de la propriété intellectuelle.

L'utilisation d'un logiciel tiers nécessaire pour l'accomplissement des missions doit faire l'objet d'une validation de la DSI avant son installation.

Section 1.9 L'utilisation de service en ligne

L'utilisateur s'engage à utiliser les services (messagerie, agenda …) mis en place par l'académie. L'utilisation de services en ligne externes est contraire aux bonnes pratiques recommandées par l'académie.

Article II- Messagerie électronique

Section 2.1 - Caractéristiques et limitations de la messagerie électronique

L'académie de Strasbourg n'exerce aucune surveillance ni aucun contrôle éditorial sur les messages envoyés dans le cadre de la messagerie électronique. L'académie ne pourra, de ce fait, en être considérée responsable.

L'utilisateur est tenu d'informer le service compétent (cellule SSI[1]) de tout message suspect ou d'utilisateurs non identifiés.

Le compte d'accès à la messagerie est constitué d'un **identifiant** et d'un **mot de passe** strictement **personnels** et **confidentiels**. L'utilisateur est responsable de leur conservation et s'engage à ne pas les divulguer et à ne pas s'approprier ceux d'un autre utilisateur. Il est nécessaire de noter que ce couple d'identifiant est également nécessaire pour accéder à la plupart des applications informatiques et des applications « métier » de l'académie de Strasbourg.

L'adresse électronique fonctionnelle ou organisationnelle peut être mise en place si elle est exploitée par un service ou un groupe d'utilisation.

L'académie de Strasbourg conserve durant une période d'une année, les entêtes (destinataire, émetteur, sujet et le nombre de pièces jointes) de tout message transmis par la messagerie électronique de l'académie.

Toutefois, il est conseillé de conserver les messages durant le temps nécessaire afin de garantir l'exercice de ses activités et de constituer un élément de preuve.

Section 2.2 – La gestion de la messagerie en cas d'absence

Lorsque l'utilisateur s'absente pour une période prolongée, afin de garantir la continuité du service, il est nécessaire d'activer le système de message de notification d'absence.

Cette activation s'opère via le webmail dans l'onglet « Option » puis « message de notification d'absence », il est nécessaire de compléter les dates du congé ainsi que le message de réponse automatique afin d'orienter l'expéditeur vers un interlocuteur habilité à assurer la correspondance.

Un guide d'utilisation de la messagerie est à votre disposition sur le site institutionnel de l'académie.

[1] Vous pouvez vous rentre sur le site de la SSI de l'académie de Strasbourg afin de signaler toute incident de sécurité sur votre poste : https://ssi.ac-strasbourg.fr/en-cas-dincident/signaler-un-incident-de-securite/

Section 2.3 : Stockage et archivage des messages

Chaque utilisateur doit organiser et assurer la conservation des messages pouvant être indispensables à l'exercice de ses activités ou simplement utiles en tant qu'éléments de preuve.

La messagerie des personnels n'est pas sauvegardée quotidiennement. Les utilisateurs doivent donc procéder à un archivage personnel.

Chaque utilisateur reste responsable de l'archivage et du classement des messages qu'il a relevés.

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

- de la périodicité de l'archivage;
- du choix des fichiers et messages conservés et de ceux qui sont détruits ;
- de la méthode et de la durée de stockage.

Article III- Mot de passe

Pour accéder aux outils informatiques, mis à disposition par l'académie de Strasbourg, l'utilisateur dispose d'identifiants qui lui sont propres et qui lui permettent de s'authentifier :

- **un compte utilisateur** (soit 1ère lettre du prénom suivi du nom d'usage soit l'adresse de la messagerie professionnelle)

- **un mot de passe** dont le changement est impératif lors de la première utilisation du poste de travail.

Section 3.1 La gestion des mots de passe

L'utilisateur s'engage à respecter la politique de gestion des mots de passe de l'académie afin de lutter contre les vols de mot de passe. Les principaux éléments à prendre en compte sont :

- d'utiliser **un mot de passe différent** du mot de passe **que vous utilisez pour vos services privés**. En particulier, l'utilisation d'un même mot de passe pour la messagerie professionnelle et pour la messagerie personnelle est à proscrire ;

- choisir un mot de passe qui n'a **aucun lien avec l'utilisateur** (mot de passe composé d'un nom de société, d'une date de naissance, etc.) ou avec un mot du dictionnaire ;

- choisir un mot de passe **comportant au moins 8 caractères, composé de lettres minuscules et majuscules, de chiffres et de caractères spéciaux :**

- Majuscules : ABCDEFGHIJKLMNOPQRSTUVWXYZ
- Minuscules : abcdefghijklmnopqrstuvwxyz
- Chiffres : 0123456789
- Caractères spéciaux : : ;:-_=\|//?^&!.@$£#*()%~<>{}[]

Pour être valable, votre mot de passe doit répondre aux critères suivants :

- Majuscules : au moins 2
- Minuscules : au moins 2
- Chiffres : au moins 2
- Caractères spéciaux AUTORISÉS : au moins 2
- Nombre de caractères : au moins 8

- ne pas demander à un tiers de générer un mot de passe préfabriqué ;

- ne pas afficher ses mots de passe (exemple sur un post-it) ;

- **modifier immédiatement les mots de passe attribués par défaut** ;

- **renouveler** les mots de passe à une fréquence raisonnable. Tous les ans, est un bon compromis pour les systèmes contenant des données professionnelles et sensibles;

- **ne jamais stocker** les mots de passe dans un fichier sur un poste informatique particulièrement exposé au risque (exemple : connecté à internet), encore moins sur un papier facilement accessible ;

L'académie de Strasbourg préconise l'utilisation du logiciel libre dénommé **Keepass** : ce logiciel est un coffre-fort numérique pour tous les mots de passe. Il permet de stocker les mots de passe dans un même et seul fichier et ceci de manière sécurisée. Néanmoins, il est important de protéger le logiciel par un mot de passe fort. Ce mot de passe ne doit pas être oublié afin de ne pas bloquer l'accès au logiciel.

- **Ne jamais communiquer** oralement, par écrit ou par mail ses identifiants et mots de passe, y compris au service informatique ;

- **ne pas communiquer** les mots de passe aux services informatiques **;**

- **configurer** les logiciels, y compris son navigateur web, pour qu'ils ne se "souviennent" pas des mots de passe.

Section 3.2 Comment changer de mot de passe ?

Il est obligatoire pour chaque utilisateur de changer le mot de passe par défaut du compte utilisateur et de messagerie. Il convient d'en changer régulièrement (une fois par an par exemple).

Pour changer le mot de passe professionnel à la messagerie, à la bureautique et au portail des applications, il devra se rendre sur le webmail.[2]

Pour toute autre question relative aux mots de passe, rendez-vous sur le site de la Sécurité des systèmes d'information. [3]

[2] https://applications.ac-strasbourg.fr/moncompte/
[3] https://ssi.ac-strasbourg.fr/

Pour plus d'informations

Le site internet

En cas de besoin d'information supplémentaire sur la charte informatique ou de déclaration d'incident liée à la sécurité de système d'information, vous pouvez vous rendre sur le site de la Sécurité des systèmes d'information de l'académie de Strasbourg au lien suivant : https://ssi.ac-strasbourg.fr/

L'assistance informatique

L'académie dispose également d'une assistance informatique, un technicien vous répond du lundi au vendredi 8h à 18h :

- Par téléphone au 0 810 000 891
- Par mail : assistance@ac-strasbourg.fr
- Via le portail Arena : http://intranet.in.ac-strasbourg.fr/
- Via le site de l'académie : www.ac-strasbourg.fr/assistance/