CHARTE REGISSANT L'USAGE DES MOYENS NUMERIQUES DE L'INSTITUT D'ETUDES POLITIQUES D'AIX EN PROVENCE

GUIDE DE L'UTILISATEUR

Table des matières

I- Préambule

Le présent guide pratique de l'utilisateur a pour objet d'accompagner les personnes utilisant les moyens numériques de l'Institut d'Etudes Politiques d'Aix-en-Provence dans la mise en œuvre des règles de sécurité et de comportement préconisées par la charte des bons usages.

Il est rédigé dans l'intérêt de chacun des utilisateurs et manifeste la volonté de l'Institut d'Etudes Politiques d'Aix-en-Provence d'assurer un développement harmonieux et sécurisé de l'accès et de l'utilisation des moyens numériques qu'il met à disposition.

Les utilisateurs sont informés que la violation des procédures décrites dans le 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 sur le site web institutionnel à l'adresse : http://www.sciencespo-aix.fr/

Rappels :

- Quels sont les « moyens numériques » ?

Les moyens numériques de l'Institut d'Etudes Politiques d'Aix-en-Provence 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'Institut d'Etudes Politiques d'Aix-en-Provence met à disposition de ses utilisateurs. ».

- Qui sont les « utilisateurs » ?

La notion d'«utilisateurs » est définie à l'article I. al. 4 de la charte comme « l'ensemble des personnes ayant obtenu l'autorisation d'accéder au système d'information de l'Institut d'Etudes Politiques d'Aix-en-Provence. ».

II- Règles de sécurité

a) Concernant la 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, messagerie électronique,…)

Les mots de passe choisis par les utilisateurs devraient être constitués de 8 caractères alphanumériques au minimum, dont au moins un chiffre ou un caractère spécial. Il est vivement recommandé de changer son mot de passe, idéalement selon une périodicité de 3 mois. Chaque utilisateur est personnellement responsable du mot de passe qu'il a choisi.

Concrètement, chaque utilisateur doit :

- choisir un mot de passe sûr, n'ayant aucun lien avec son environnement familier ;
- changer de mot de passe régulièrement ;
- 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.

b) Paramétrage des postes de travail

1- Principes généraux

Le poste de travail de l'utilisateur constitue un outil qui doit être protégé des intrusions. A 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.

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

Qu'est-ce qu'un anti-virus ?

Un anti-virus est un logiciel de protection dont le but est de détecter les virus ou logiciels malveillants. 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.

Qu'est-ce qu'un pare feu ?

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

Il est indispensable de le maintenir car il représente une des principes protections actives des postes sur le réseau.

3- 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.

4- Les périphériques de stockage

Les périphériques de stockages comme les clés USB, les disques durs externes, les cartes mémoires – 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 son propriétaire. Il est donc conseillé de :

- privilégier son propre périphérique pour un échange de données, plutôt que d'utiliser un matériel d'origine inconnue,
- d'une manière générale, il est recommandé de séparer les usages entre les périphériques de stockages professionnels et privés.

  Exemple : ne pas utiliser d'outils de type *Gmail*, *Yahoo*, *Skype* ou *Dropbox* pour des échanges professionnels. Des outils similaires sont proposés dans votre environnement numérique de travail (messagerie, échanges de fichiers…)

c) Messagerie électronique

1- Messages à caractère privé

RAPPEL : aux termes de la charte du bon usage des moyens numériques de l'IEP d'Aix-en-Provence (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 et le personnel administratif, technique de l'Institut d'Etudes Politiques d'Aix en Provence) ou détachés des activités pédagogiques (pour les utilisateurs étudiants). Les utilisateurs doivent alors :

- dans le cadre d'un message à caractère strictement privé, reçu ou émis, faire mentionner en objet la mention « Privé », afin d'exprimer sans ambiguïté le caractère extra-professionnel du message
- seront alors réputés professionnels les messages ne comportant pas, en objet, cette mention.

2- Caractéristiques et limitations de la messagerie électronique

Parmi ses fonctionnalités, la messagerie électronique permet l'échange de fichiers en « pièces jointes ». L'émission, comme la réception, de messages contenant des pièces jointes est limitée à un usage raisonnable de cette fonctionnalité. L'usage est raisonnable lorsque :

- la taille des fichiers joints, en émission ou réception, est limitée et compatible avec le bon fonctionnement du service messagerie ;
- la fonctionnalité est utilisée principalement à des fins professionnelles.

Pour prévenir les abus, les messages émis ou reçus font l'objet d'une limitation technique de non distribution. 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 message 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 entraîne le blocage, chez les prestataires, de tous les messages en provenance de l'Institut d'Etudes Politique d'Aix-en-Provence. Pour prévenir de tels dysfonctionnements, une limite technique est mise en œuvre par la direction du Système d'Information et Stratégie 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, qui ne provoquent aucunes perturbations.

3- 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'Institut d'Etudes Politique d'Aix-en-Provence est sauvegardée quotidiennement, ce qui ne dispense en aucun cas les utilisateurs de procéder à un archivage personnel.

Cela signifie que, malgré ce stockage sur le serveur de messagerie de l'Institut d'Etudes Politique d'Aix-en-Provence, 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 :

- 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.

4- 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 informatique, de codes malveillants, susceptibles d'entraîner des conséquences d'une extrême gravité pour l'Institut d'Etudes Politique d'Aix-en-Provence.

Les utilisateurs sont informés que l'Institut d'Etudes Politique d'Aix-en-Provence 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 vérifier qu'ils ne comportent pas de virus.

D'une manière générale 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 des Système d'Information et Stratégie Numérique.

d) Navigation sur Internet

Il est rappelé que l'accès à Internet n'est autorisé qu'au travers des dispositifs de sécurité mis en place par l'Institut d'Etudes Politique d'Aix-en-Provence.

Les utilisateurs ne doivent recourir qu'aux navigateurs sélectionnés et qualifiés par le Direction des Systèmes d'Information et Stratégie numérique (SISN), en respectant ses préconisations sur leur paramétrage et en privilégiant les extensions (plugins et modules complémentaires) recommandées par l'Institut d'Etudes Politique d'Aix-en-Provence

Certains sites malveillants profitent des failles des navigateurs 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.

Il convient de faire preuve de prudence, 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.

Navigation privée
Les utilisateurs sont invités à privilégier la navigation en mode « privé », option disponible sur tous les navigateurs proposés par la SISN.

Ce mode limite le stockage des données de navigation. Il évite ainsi la conservation d'informations personnelles, dont les mots de passe, dans la mémoire du navigateur. Concrètement, il permet de supprimer les « témoins de connexion » ou « cookies », susceptibles d'engendrer des risques pour la sécurité des informations personnelles, notamment lorsque plusieurs utilisateurs ont accès au même poste.

e) Sauvegarde données : quelques repères

- L'Institut d'Etudes Politique d'Aix-en-Provence organise une sauvegarde des données sur un ensemble de postes informatiques (notamment ceux connectés au réseau « administratif »).

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

f) Matériel nomade

1- 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'Institut d'Etudes Politique d'Aix-en-Provence, 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 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.

L'accès au réseau local est réservé au matériel confié par l'Institut d'Etudes Politiques d'Aix-en-Provence, aucun autre matériel ne doit y être connecté.

2- 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 de l'Institut d'Etudes Politique d'Aix-en-Provence 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 de l'Institut d'Etudes Politique d'Aix-en-Provence par l'intermédiaire du support informatique dont les coordonnées sont rappelées plus bas.

3- Détérioration

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

g) Les règles déplacement : en cas d'absences, départs ou mutations

Aux termes de l'article II.2 de la charte de bonne utilisation des moyens numériques, il appartient à tout membre du personnel, quittant à titre provisoire ou définitif l'Institut d'Etudes Politique d'Aix-en-Provence, 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.

1- Suppression des données privées

L'attention des agents et des enseignants de l'Institut d'Etudes Politique d'Aix-en-Provence 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'Institut d'Etudes Politique d'Aix-en-Provence 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.

2- Préparer son absence

Au-delà de la suppression des données privées, il convient également de :

- demander la suppression des accès aux logiciels, applications de travail (SIFAC, SOSIE, …) ;
- s'assurer de la mise en place d'un « répondeur » sur la messagerie électronique, orientant les demandeurs vers un autre contact ;
- faire retirer l'adresse électronique professionnelle des différentes listes de diffusion.

III- Pour en savoir plus

a) Liens utiles

- **ANSSI** (Agence Nationale de la Sécurité des Systèmes d'information) :*http://www.ssi.gouv.fr/*
- **Portail de la Sécurité Informatique** : *http://www.securite-informatique.gouv.fr/*
- **CERTA, Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques** : *http://www.certa.ssi.gouv.fr/*

b) Exemples de logiciels utiles et gratuits

- **VeraCrypt** : logiciel de chiffrage pour Windows et Linux.
- **OpenVPN** : client VPN pour Windows et Linux.
- **Putty** : pour accéder à des serveurs Linux de façon sécurisée.
- **Thunderbird** : client de messagerie.
- **Firefox** : navigateur web.
- **LibreOffice** : suite bureautique compatible avec tous les systèmes.
- **Ccleaner et MalWareBytes:** nettoyeur de fichiers temporaires.

IV- Besoin d'aide ?

a) Assistance

En cas de besoin d'assistance ou de renseignements complémentaires, vous pouvez adresser vos demandes au support informatique de l'Institut d'Etudes Politiques d'Aix en Provence en écrivant à l'adresse suivante : informatique@sciencespo-aix.fr

b) Données personnelles

Le contact privilégié pour l'exercice des droits reconnus par la loi « Informatique et Libertés » et pour toutes les questions relatives à la protection des données à caractère personnel, est : informatique@sciencespo-aix.fr