Charte informatique

Axis et ses filiales

Pour toutes questions complémentaires
Flavien MAILLOT « flavien@axis-immobilier.com »

Table des matières

I. INTRODUCTION

Axis met en œuvre un système d'information et de communication nécessaire à l'exercice de son activité. Elle met ainsi à disposition de ses collaborateurs des outils informatiques, et de communication.

La présente charte concerne les ressources informatiques, les services internet, de messagerie et téléphoniques de l'entreprise Axis, ainsi que tout autre moyen de connexion à distance permettant d'accéder, via le réseau informatique, aux services de communication ou de traitement électronique interne ou externe. Il s'agit principalement des outils suivants : ordinateurs portables et fixes, tablettes tactiles, téléphones portables et fixes, imprimantes, logiciels.
Elle a également pour objet de sensibiliser les utilisateurs aux risques liés à l'utilisation de ces ressources en termes d'intégrité et de confidentialité des informations traitées. Ces risques imposent le respect de certaines règles de sécurité et de bonne conduite. L'imprudence, la négligence ou la malveillance d'un utilisateur peuvent en effet avoir des conséquences graves de nature à engager sa responsabilité civile et / ou pénale ainsi que celle de la société ou ses filiales.

Le cadre règlementaire de la sécurité de l'information est complexe. Chaque membre du personnel se doit de respecter les règles juridiques applicables, notamment en matière :

- de respect des règles déontologiques et professionnelles,
- de respect des procédures de travail,
- de respect de l'organisation et des règles de délégation,
- de communication d'informations,
- d'utilisation des moyens informatiques mis à sa disposition dans le cadre de sa fonction.

L'utilisation de l'informatique est encadrée par une législation très stricte visant à protéger d'une part les atteintes aux droits de la personne résultant de l'utilisation des fichiers ou traitements informatiques, d'autre part les atteintes aux systèmes de traitement automatisé de données.

Par ailleurs, le Code de la Propriété Intellectuelle protège le droit de propriété attaché aux logiciels et aux données (textes, images et sons).

II. PROTECTION DES DONNÉES À CARACTERE PERSONNEL

La loi n°78-17 du 6 janvier 1978 modifiée en 2004 relative à l'informatique, aux fichiers et aux libertés définit les conditions dans lesquelles des traitements de données à caractère personnel peuvent être effectués. Elle ouvre aux personnes concernées par les traitements un droit d'accès et de rectification des données enregistrées sur leur compte.

Axis a désigné un correspondant à la protection des données à caractère personnel. Ce dernier a pour mission de veiller au respect des dispositions de la loi n°78-17 du 6 janvier 1978 modifiée.

Il est obligatoirement consulté par le responsable des traitements préalablement à leur création.

Il recense dans un registre la liste de l'ensemble des traitements de données à caractère personnel d'Axis au fur et à mesure de leur mise en œuvre. Cette liste est tenue à disposition de toute personne en faisant la demande. Elle est également diffusée sur l'intranet d'Axis.

Le correspondant veille au respect des droits des personnes (droit d'accès, de rectification et d'opposition). En cas de difficultés rencontrées lors de l'exercice de ces droits, les personnes concernées peuvent saisir le correspondant, directeur des nouvelles technologies, Flavien MAILLOT si@axis-immobilier.com.

III. LE CHAMP D'APPLICATION DE LA CHARTE

La présente charte s'applique à tout utilisateur du Système d'Information et de communication d'Axis pour l'exercice de ses activités professionnelles. L'utilisation à titre privé de ces outils est tolérée, mais doit être raisonnable et ne pas perturber le bon fonctionnement du service.

La charte est diffusée à l'ensemble des utilisateurs par note de service et, à ce titre, mise à disposition sur l'intranet (http://intraaaxis.com) de Axis. Elle est remise à tout nouvel arrivant. Elle est disponible dans sa dernière version papier dans le pôle informatique.

Quelques définitions :
On désignera sous le terme « utilisateur » toute personne autorisée à accéder aux outils informatiques et aux moyens de communication d'Axis et à les utiliser : employés, stagiaires, intérimaires, personnels de sociétés prestataires, visiteurs occasionnels....

Les termes "outils informatiques et de communication" recouvrent tous les équipements informatiques, de télécommunications et de reprographie d'Axis.

IV. LES RÈGLES D'UTILISATION DU SYSTEME D'INFORMATION D'AXIS

Chaque utilisateur accède aux outils informatiques nécessaires à l'exercice de son activité professionnelle dans les conditions définies par Axis.

1. Les modalités d'intervention du service de l'informatique interne

Le service de l'informatique interne de la commission assure le bon fonctionnement et la sécurité des réseaux, des moyens informatiques et de communication d'Axis. Les agents/personnels de ce service disposent d'outils techniques afin de procéder aux investigations et au contrôle de l'utilisation des systèmes informatiques mis en place.

Ils ont accès à l'ensemble des données techniques mais s'engagent à respecter les règles de confidentialité applicables aux contenus des documents.

Ils sont assujettis au devoir de réserve et sont tenus de préserver la confidentialité des données qu'ils sont amenés à connaître dans le cadre de leurs fonctions.

Compte tenu de la nature des fonctions du directeur des nouvelles technologies, il est sensibilisé à la confidentialité, mais aussi au plus grand secret professionnel.

2. L'authentification

Les ressources informatiques sont segmentées. Les deux ressources principales reposent sur l'utilisation d'un nom de compte ("login" ou identifiant) fourni à l'utilisateur lors de son arrivée chez Axis. Un mot de passe est associé à cet identifiant de connexion.

Les moyens d'authentification sont personnels et confidentiels.

Actuellement, le mot de passe doit être composé de 8 caractères minimum combinant chiffres, lettres et caractères spéciaux. Il ne doit comporter ni le nom, prénom ni l'identifiant d'ouverture de la session de travail. Il doit être renouvelé régulièrement.

3. Les règles de sécurité

Tout utilisateur s'engage à respecter les règles de sécurité suivantes :

- Signaler au service informatique interne d'Axis toute violation ou tentative de violation suspectée de son compte réseau et de manière générale tout dysfonctionnement.
- Ne jamais confier son identifiant/mot de passe.
- Ne jamais demander son identifiant/mot de passe à un collègue ou à un collaborateur.
- Ne pas masquer sa véritable identité.
- Ne pas usurper l'identité d'autrui.
- Ne pas modifier les paramétrages du poste de travail.
- Ne pas installer de logiciels sans autorisation.
- Ne pas copier, modifier, détruire les logiciels propriétés de Axis.
- Verrouiller son ordinateur dès qu'il quitte son poste de travail.
- Ne pas accéder, tenter d'accéder, supprimer ou modifier des informations qui ne lui appartiennent pas.
- Toute copie de données sur un support externe est soumise à l'accord du supérieur hiérarchique et doit respecter les règles définies par Axis.

En outre, il convient de rappeler que les visiteurs ne peuvent avoir accès au Système d'Information d'Axis sans l'accord préalable du service informatique interne.

Les intervenants extérieurs doivent s'engager à faire respecter la présente charte par leurs propres salariés et éventuelles entreprises sous-traitantes. Dès lors, les contrats signés entre Axis et tout tiers ayant accès aux données, aux programmes informatiques ou autres moyens, doivent comporter une clause rappelant cette obligation.

V. LES MOYENS INFORMATIQUES

1. Configuration du poste de travail

Dans la mesure où l'utilisateur n'a pas la possibilité d'amener son propre ordinateur. Axis met à disposition de chaque utilisateur un poste de travail doté des outils informatiques nécessaires à l'accomplissement de ses fonctions.
L''utilisateur ne doit pas :

- Modifier ces équipements et leur fonctionnement, leurs paramétrages, ainsi que leurs configurations physiques ou logicielles.
- Connecter ou déconnecter du réseau les outils informatiques et de communications sans y avoir été autorisé par l'équipe informatique interne.
- Déplacer l'équipement informatique (sauf s'il s'agit d'un « équipement nomade »)
- Nuire au fonctionnement des outils informatiques et de communications.

Toute installation de logiciels supplémentaires (logiciels de consultation de fichiers multimédia) est subordonnée à l'accord du service informatique interne.

2. Équipements nomades et procédures spécifiques aux matériels de prêt.

Équipements nomades

On entend par « **équipements nomades** » tous les moyens techniques mobiles (ordinateur portable, imprimante portable, téléphones mobiles ou smartphones, CD ROM, clé USB etc.…).

Quand cela est techniquement possible, ils doivent faire l'objet d'une sécurisation particulière, au regard de la sensibilité des documents qu'ils peuvent stocker, notamment par chiffrement.

Quand un ordinateur portable se trouve dans le bureau de l'agent qui en a l'usage, cet ordinateur doit être physiquement sécurisé de la meilleure façon qui est mise à disposition (sauf quand l'utilisateur est physiquement présent dans son bureau).

L'utilisation de smartphones pour relever automatiquement la messagerie électronique comporte des risques particuliers pour la confidentialité des messages, notamment en cas de perte ou de vol de ces équipements. Quand ces appareils ne sont pas utilisés pendant quelques minutes, ils doivent donc être verrouillés par un moyen adapté de manière à prévenir tout accès non autorisé aux données qu'ils contiennent.

Procédures spécifiques aux matériels de prêt

L'utilisateur doit renseigner et signer un registre, tenu par le service informatique interne, ou le service en charge, actant la remise de l'équipement nomade ou encore la mise à disposition d'un matériel spécifique pour la tenue d'une réunion (vidéoprojecteur). Il en assure la garde et la responsabilité et doit informer la direction compétente ainsi que le directeur des nouvelles technologies en cas d'incident (perte, vol, dégradation) afin qu'il soit procédé aux démarches telles que la déclaration de vol ou de plainte. Il est garant de la sécurité des équipements qui lui sont remis et ne doit pas contourner la politique de sécurité mise en place sur ces mêmes équipements. Le retour du matériel est consigné dans le registre.

3. Internet

Les utilisateurs peuvent consulter les sites internet présentant un lien direct et nécessaire avec l'activité professionnelle, de quelque nature qu'ils soient.

Toutefois, une utilisation ponctuelle et raisonnable, pour un motif personnel, des sites internet dont le contenu n'est pas contraire à la loi, l'ordre public, et ne met pas en cause l'intérêt et la réputation de l'institution, est admise.

4. Messagerie électronique

Conditions d'utilisation

La messagerie mise à disposition des utilisateurs est destinée à un usage professionnel. L'utilisation de la messagerie à des fins personnelles est tolérée si elle n'affecte pas le travail de l'agent ni la sécurité du réseau informatique d'Axis.

Tout message qui comportera la mention expresse ou manifeste de son caractère personnel bénéficiera du droit au respect de la vie privée et du secret des correspondances. À défaut, le message est présumé professionnel.

Axis s'interdit d'accéder aux dossiers et aux messages identifiés comme « personnel » dans l'objet de la messagerie de l'agent.

L'utilisation de la messagerie électronique doit se conformer aux règles d'usage définies par le service informatique interne, et validées par le directeur des nouvelles technologies.

Le transfert de messages, ainsi que leurs pièces jointes, à caractère professionnel sur des messageries personnelles est soumis aux mêmes règles que les copies de données sur supports externes.

Les agents peuvent consulter leur messagerie à distance, à l'aide d'un navigateur (Webmail). Les fichiers qui seraient copiés sur l'ordinateur utilisé par l'agent dans ce cadre doivent être effacés dès que possible de l'ordinateur utilisé.

Consultation de la messagerie

En cas d'absence d'un agent et afin de ne pas interrompre le fonctionnement du service, le service informatique interne d'Axis peut, ponctuellement transmettre au supérieur hiérarchique un message électronique à caractère exclusivement professionnel et identifié comme tel par son objet et/ou son expéditeur (cf conditions d'utilisation).

Le supérieur hiérarchique n'a pas accès aux autres messages de l'agent. L'agent concerné est informé dès que possible de la liste des messages qui ont été transférés.

En cas d'absence prolongée d'un agent (longue maladie), le chef de service peut demander au service informatique, après accord de son directeur, le transfert des messages reçus.

Courriel non sollicité

Axis dispose d'un outil permettant de lutter contre la propagation des messages non désirés (spam). Aussi, afin de ne pas accentuer davantage l'encombrement du réseau lié à ce phénomène, les utilisateurs sont invités à limiter leur consentement explicite préalable à recevoir un message de type

commercial, newsletter, abonnements ou autres, et de ne s'abonner qu'à un nombre limité de listes de diffusion notamment si elles ne relèvent pas du cadre strictement professionnel.

5. Téléphone

Si nécessaire, Axis met à disposition des utilisateurs, pour l'exercice de leur activité professionnelle, des téléphones fixes et mobiles.

L'utilisation du téléphone à titre privé est admise à condition qu'elle demeure raisonnable.

Des restrictions d'utilisation par les agents des téléphones fixes sont mises en place en tenant compte de leurs missions. À titre d'exemple, certains postes sont limités aux appels nationaux, d'autres peuvent passer des appels internationaux.

Axis s'interdit de mettre en œuvre un suivi individuel de l'utilisation des services de télécommunications. Seules des statistiques globales sont réalisées sur l'ensemble des appels entrants et sortants. Elle vérifie que les consommations n'excèdent pas les limites des contrats passés avec les opérateurs.

Axis s'interdit d'accéder à l'intégralité des numéros appelés via l'autocommutateur mis en place et via les téléphones mobiles. Toutefois, en cas d'utilisation manifestement anormale, le service informatique, sur demande du Directeur administratif et financier (Mikael Hadjedj), ou du Directeur général (Benoit Jobert, Matthieu Brugières), se réserve le droit d'accéder aux numéros complets des relevés individuels.

VI. L'ADMINISTRATION DU SYSTEME D'INFORMATION

Afin de surveiller le fonctionnement et de garantir la sécurité du système d'information, différents dispositifs sont mis en place.

1. Les systèmes automatiques de filtrage

À titre préventif, des systèmes automatiques de filtrage permettant de diminuer les flux d'information pour Axis et d'assurer la sécurité et la confidentialité des données sont mis en œuvre, par le directeur des nouvelles technologies. Il s'agit notamment du filtrage des sites Internet, de l'élimination des courriels non sollicités, du blocage de certains protocoles (Peer to Peer, messagerie instantanée…).

2. Les systèmes automatiques de traçabilité

Le directeur des nouvelles technologies de Axis opère sans avertissement les investigations nécessaires à la résolution de dysfonctionnements du système d'information ou de l'une de ses composantes, qui mettent en péril son fonctionnement ou son intégrité.

Il s'appuie pour ce faire, sur des fichiers de journalisation (fichiers « logs ») qui recensent toutes les connexions et tentatives de connexions au système d'information. Ces fichiers comportent les données nécessaires à l'identification de la personne.
Le service informatique est le seul utilisateur de ces informations.

3. Gestion du poste de travail

À des fins de maintenance informatique, le service informatique interne d'Axis, peut accéder à distance à l'ensemble des postes de travail. Cette intervention s'effectue avec l'autorisation expresse de l'utilisateur.

Dans le cadre de mises à jour et évolutions du système d'information, et lorsqu'aucun utilisateur n'est connecté sur son poste de travail, le service informatique peut être amené à intervenir sur l'environnement technique des postes de travail. Il s'interdit d'accéder aux contenus.

Dans le cadre du renforcement de la sécurité informatique, le directeur des nouvelles technologies d'Axis peut accéder à des équipements (nomades ou non) présents sur le réseau. Il s'interdit d'accéder aux contenus, il est soumis au secret professionnel et il s'engage à tout mettre en œuvre pour corriger les failles de sécurités. Même sur demande express ces manœuvres ne seront pas exercées dans un cadre autre que celui définit.

4. Navigation sur le WEB

L'utilisateur est informé que les traces de la navigation sont temporairement archivées. En effet, à la demande d'une autorité judiciaire ou administrative, le directeur des nouvelles technologies devra fournir les informations de la navigation web.
Il se réserve le droit :

- de contrôler le contenu de toute page Web en vue de s'assurer du respect des conditions d'utilisation des services énoncées par la présente Charte

5. Contrôle d'accès

Axis a mis en place un système d'accès par badge pour contrôler l'accès à ses locaux.
Nous enregistrons les données nécessaires à l'identification de la personne pendant la durée légale autorisée.

Les destinataires des données sont uniquement les personnels légalement habilités, à savoir le directeur des nouvelles technologies et les personnels de la société en charge de la maintenance du matériel, à cette seule fin.

Sur motivation, une copie peut être communiqué de façon légale aux Directeurs Généraux (Matthieu Brugieres, Benoit Jobert) ainsi qu'au directeur d'exploitation de la résidence concernée.

6. Vidéosurveillance

Axis a placé ses locaux sous vidéosurveillance afin d'assurer la sécurité de son personnel, de ses biens et de ses autres utilisateurs. Les images enregistrées dans ce dispositif ne sont pas utilisées à des fins de surveillance du personnel ni de contrôle des horaires.

La base légale du traitement est l'intérêt légitime (cf. article 6.1.f) du Règlement européen sur la protection des données.
Les employés de la société Axis et de ses filiales, les visiteurs occasionnels et régulier des locaux de la société sont filmés par le dispositif.

Les images sont conservées le temps légal.

En cas d'incident lié à la sécurité des personnes et des biens, les images de vidéosurveillance peuvent néanmoins être extraites du dispositif. Elles sont alors conservées sur un autre support le temps du règlement des procédures liées à cet incident et accessibles aux seules personnes habilitées dans ce cadre.

Des mots de passes temporaires vont être mis en place à l'attention du Directeur Général dans le cadre de l'analyse des flux de personnes.

7. Géolocalisation des équipements nomades

Axis et ses filiales, ont la possibilité localiser certains de leurs équipements nomades aux fins d'optimiser la couverture réseau, les services fournis au sein de ses établissements et de protéger ses employés en cas de perte ou de vol. De façon subsidiaire, d'augmenter la sureté ou la sécurité de l'employé lui-même lors de ses déplacements. Le système n'a pas pour objet le suivi du temps de travail des salariés et ne permet pas davantage de contrôler les déplacements en-dehors du temps de travail.
La durée de conservation des données est celle définie par la CNIL à savoir deux mois.

Seul le directeur des nouvelles technologies traite ces données lorsque les circonstances l'imposent.

VII. DROIT À LA DÉCONNEXION

Le droit à la déconnexion s'entend comme le droit de chaque salarié de ne pas répondre aux courriels et autres messages en dehors des heures de travail, afin de garantir l'équilibre entre vie professionnelle et vie privée, les temps de repos et de récupération, de réguler la charge mentale et réduire les risques de burn-out.

Le droit à la déconnexion dans l'entreprise fait l'objet d'un accord d'entreprise dans le cadre de la négociation annuelle sur l'égalité professionnelle entre les hommes et les femmes et la qualité de vie au travail.

VIII. PROCÉDURE APPLICABLE LORS DU DÉPART DE L'UTILISATEUR

Lors de son départ, l'utilisateur doit restituer au service de l'informatique interne les matériels mis à sa disposition.

Il doit préalablement effacer ses fichiers et données privées. Toute copie de documents professionnels doit être autorisée par le chef de service.

Les données personnelles de l'utilisateur sont, en tout état de cause, supprimés dans un délai maximum d'un mois après son départ, sauf les données nécessaires à répondre à des demandes relevant de la règlementation légale.

IX. RESPONSABILITÉS- SANCTIONS

Le manquement aux règles et mesures de sécurité et de confidentialité définies par la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner des sanctions à son encontre.

Des sanctions en interne peuvent être prononcées, elles consistent :

- dans un premier temps, en un rappel à l'ordre émanant du service informatique interne, après avis du directeur des nouvelles technologies, en cas de non-respect des règles énoncées par la charte ;
- dans un second temps, et en cas de renouvellement, après avis du directeur des nouvelles technologies et du supérieur hiérarchique, en des sanctions disciplinaires.
- Le non-respect des lois et textes applicables en matière de sécurité des systèmes d'information (cf. liste des textes en annexe) est susceptible de sanctions pénales prévues par la loi.

X. ENTRÉE EN VIGUEUR DE LA CHARTE

Elle est applicable à compter du 01/07/2018

Le Directeur des Nouvelles Technologies
MAILLOT Flavien

Annexe

DISPOSITIONS LÉGALES APPLICABLES

Directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiées par la loi n°2004-801 du 6 août 2004.
Dispositions Pénales :

- Code Pénal (partie législative) : art 226-16 à 226-24
- Code Pénal (partie réglementaire) : art R. 625-10 à R. 625-13

Loi n°88-19 du 5 janvier 1988 relative à la fraude informatique dite loi Godfrain. Dispositions pénales : art 323-1 à 323-3 du Code pénal.

Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN)

Loi n°94-361 du 10 mai 1994 sur la propriété intellectuelle des logiciels. Disposition pénale : art L.335-2 du Code pénal.