

**NC3 Services**

**Eléments principaux composant**

**une charte**

**Sécurité de l’information**

**Informations générales**

Version : 4

État document : Draft

Document : Eléments principaux composant une charte – Sécurité de l’information

Date : 11/12/2019

Représentant :

Table des matières

[1 Objet de la charte 3](#_Toc479843810)

[2 Engagement de la direction 3](#_Toc479843811)

[3 Champ d’application et sanctions 4](#_Toc479843812)

[4 Usage des systèmes d'information 4](#_Toc479843813)

[5 Gestion des mots de passe 4](#_Toc479843814)

[5.1 Responsabilité des employés 4](#_Toc479843815)

[5.2 Création de mots de passe 5](#_Toc479843816)

[5.3 Pérennité des mots de passe 5](#_Toc479843817)

[5.4 Sauvegarde des mots de passe 5](#_Toc479843818)

[6 Utilisation du matériel électronique 6](#_Toc479843819)

[6.1 BYOD 6](#_Toc479843820)

[6.1.1 Responsabilités 6](#_Toc479843821)

[6.1.2 Devoirs 6](#_Toc479843822)

[6.2 Utilisation des ordinateurs de bureau 6](#_Toc479843823)

[6.3 Utilisation d'un Laptop ou d'un Smartphone 7](#_Toc479843824)

[6.3.1 Règles communes d’un Laptop ou d'un Smartphone 7](#_Toc479843825)

[6.3.2 Règles spécifiques aux Laptops 7](#_Toc479843826)

[6.3.3 Règles spécifiques aux Smartphone 8](#_Toc479843827)

[6.4 Installation de logiciel 8](#_Toc479843828)

[6.5 Utilisation de l'accès à distance de la société 8](#_Toc479843829)

[7 Usage des services Internet (Web) 9](#_Toc479843830)

[8 Gestion des emails 9](#_Toc479843831)

[8.1 Création d'un compte 9](#_Toc479843832)

[8.2 Utilisation du courrier électronique 9](#_Toc479843833)

[8.3 Prérogatives à l’envoi d’email 10](#_Toc479843834)

[8.4 Sauvegarde des emails 10](#_Toc479843835)

[8.5 Effacement des emails volumineux non professionnels 10](#_Toc479843836)

[8.6 Utilisation défendue des emails 11](#_Toc479843837)

[8.7 Utilisation de la signature électronique 11](#_Toc479843838)

[8.8 Utilisation du chiffrement 11](#_Toc479843839)

[8.9 Sécurité et événements de sécurité 11](#_Toc479843840)

[8.10 Décharge et signature 11](#_Toc479843841)

[9 Gestion des clés et des badges 12](#_Toc479843842)

[10 Bureau propre 12](#_Toc479843843)

[11 Mise au rebut 12](#_Toc479843844)

Nature du document

Ce document est une aide à la création d’une Politique/Charte de sécurité de l’information. Il reprend les grandes lignes des bonnes pratiques et consignes devant être respectées par les employés d’un organisme. Les informations contenues dans ce document ne sont pas exhaustives et devrons toujours être personnalisées à l’organisme receveur, sachant qu’une bonne pratique peut être acceptée, adaptée ou même rejetée selon le contexte.

Voici deux bonnes pratiques fondamentales :

* **écrire ce que l’on veut faire, pour ensuite faire « TOUT » ce que l’on a écrit ;**
* **Mieux vaut en écrire moins et en appliquer l’entièreté, que de vouloir être exhaustif et d’en appliquer qu’une partie.**

# Objet de la charte

La présente charte est un code de bonnes pratiques qui permet d’utiliser le système d’informations dans les meilleures conditions de sécurité, d’une manière confiante et responsable et dans le respect d’autrui.

Elle expose également les droits et obligations qui découlent de l’engagement réciproque entre l’employé et la société.

# Engagement de la direction

Notre société met en œuvre cette Politique/Charte, afin de définir les règles de sécurité de l’information devant être respectées par toutes les personnes travaillant pour elle.

Nous nous engageons ainsi à soutenir toutes les actions qui s’inscrivent dans le cadre de la sécurité de l’information et à mettre à disposition les moyens nécessaires à leur réalisation.

Toute personne travaillant dans notre société, se doit de suivre cette démarche :

* en prenant connaissance et en appliquant les présentes mesures dans son domaine d’activités respectif ;
* en informant les différentes parties, telles que collègues et contacts externes, des règles qui leur sont applicables.

Les manquements aux mesures de sécurité de l’information seront sanctionnés.

<la\_direction>

# Champ d’application et sanctions

La présente charte s’applique à l’ensemble des employés de la société tous statuts confondus, et plus généralement à l’ensemble des personnes, permanentes ou temporaires, utilisant les moyens informatiques de la société.

Elle sera en outre communiquée et signée les personnes entrant dans le champ d’application cité ci-dessus.

Le non-respect intentionnel, unique ou répété, de règles de la présente charte, des infractions flagrantes aux articles du code pénal, aux lois sur la protection de la vie privée, ainsi que tout non-respect du droit de la propriété intellectuelle pourront entraîner des sanctions disciplinaires qui tiendront compte d’une par des risques encourus et d’autre par des dommages subis.

Dans le cas de violations graves aux lois et législations, la direction pourra être amenée à saisir les instances judiciaires.

# Usage des systèmes d'information

Les moyens mis à disposition des employés de la société sont destinés à un usage professionnel. Néanmoins, la société reconnaît un droit d'usage privé, lorsque celui-ci est justifié par un intérêt acceptable, si l’utilisation reste dans des limites raisonnables et si l’employé se comporte de façon responsable. L'utilisation des ressources professionnelles à titre privé doit suivre le principe "du bon père de famille" et doit respecter les règles suivantes :

* il est interdit d'utiliser les ressources de la société à des fins qui pourraient nuire à l’intégrité de personnes physiques ou morales ou encore pour l’image de la société ;
* la législation en vigueur est connue de tous et appliquée.
* l'usage des ressources à titre privé ne doit occasionner aucun trouble ou dysfonctionnement du travail des autres utilisateurs ;
* les employés ne peuvent sans autorisation préalable, outrepasser les droits et autorisations qui leur ont été attribués, c'est-à-dire modifier, reproduire, détruire ou lire des informations qui ne leur sont pas destinées ;
* collaborer avec les personnes du service informatique, afin de faciliter l'identification et la correction de problèmes ou d'anomalies pouvant se présenter ;
* le matériel mis à disposition du personnel sera utilisé, manipulé ou stocké avec les soins nécessaires pour éviter toute détérioration ;
* il est interdit de connecter des supports amovibles provenant ou ayant été connectés à des sources externes, à quelconque appareil de la société, sans avoir effectué le contrôle d'usage mis en œuvre par le service informatique ;
* les employés ne peuvent sans autorisation préalable, sortir du matériel ou de l’information de l’enceinte de la société.

# Gestion des mots de passe

## Responsabilité des employés

L’employé est personnellement responsable de la protection adéquate de son mot de passe. Le mot de passe est une information secrète, personnelle qui ne doit jamais être transmise.

## Création de mots de passe

Les mots de passe utilisés au sein de la société sont strictement personnels et doivent respecter les règles minimales suivantes :

* avoir une longueur minimale de 12 caractères ;
* être composé de lettres majuscules, minuscules et de chiffres.

Une dérogation existe toutefois, pour les systèmes n’acceptant pas ces contraintes (code PIN d’un Smartphone, par exemple).

Il est strictement interdit :

* de garder au-delà de la première utilisation, les mots de passe attribués par défaut par le responsable du système concerné ;
* d’utiliser des mots de passe facile à deviner (nom de l’utilisateur, le nom d’un animal domestique, une date de naissance, un numéro de téléphone, etc.) ;
* d’utiliser des mots d’un dictionnaire (aussi étranger), des noms de villes ou de pays ou encore de mois ;
* d’utiliser le mot de passe attribué par le service informatique ;
* d’utiliser un mot de passe basé sur l’identifiant de l’utilisateur ;
* d’utiliser le même mot de passe pour plusieurs systèmes ;
* de donner son mot de passe à un collègue, un supérieur ou au service informatique ;
* de noter le mot de passe sans pour autant le protéger de la façon convenable ;
* d’envoyer ou de divulguer un mot de passe par email, téléphone, Internet, etc.

Il est conseillé de créer le mot de passe de la manière suivante :

* choisir une phrase d’un poème, d’un film ou d’une autre source bien connue ;
* prendre ensuite la première ou la deuxième lettre ;
* changer par exemple, les lettres « S » en le chiffre « 5 », « l » en « 1 » ou encore « o » en « 0 ».

Exemple: *« il est difficile de changer une opinion bien ancrée! »* donne : *« 1eddcuobA! »*

Pour ne pas utiliser le même mot de passe pour chaque système, vous pouvez le changer en jouant sur plusieurs lettres ou en insérant des signes non alphanumériques :

"2eddcuobB!", "3eddcuobA?", "3eddc,uobA?"

## Pérennité des mots de passe

Les mots de passe doivent être changés de façon régulière :

* Tous les mots de passe type administrateur doivent être changés tous les 6 mois au minimum ;
* Tous les autres mots de passe doivent être changés au moins tous les ans ;
* Au moindre soupçon de compromission, le mot de passe du système concerné doit être immédiatement changé.

## Sauvegarde des mots de passe

Les mots de passe :

* de type « administrateur », ou
* de par leur nature devant être utilisés par plusieurs personnes, ou encore
* donnant accès à des documents chiffrés,

sont sauvegardés dans une liste prévue à cet effet et sous la responsabilité du responsable informatique.

Cette liste doit uniquement exister sous forme papier, enfermée dans une enveloppe scellée et être déposée dans une armoire coupe-feu. Les personnes en droit d’y accéder et d’utiliser cette liste sont désignées par le responsable informatique.

Les mots de passe « normaux » peuvent aussi être sauvegardés par des programmes prévus à cet effet (KeePass, par exemple).

# Utilisation du matériel électronique

## BYOD

L’accès BYOD est attribué aux employés ayant un besoin professionnel motivé d’accéder aux services de la société à partir d’un équipement privé.

L’accès aux services de la société peut être limité ou bloqué dans le cas ou des anomalies seraient constatées.

Il est de la responsabilité de l’employé de s’assurer que son appareil est compatible avec les contraintes techniques de l’accès mobile proposé. Ni l’employeur, ni le fournisseur du service ne peuvent être contraints à supporter l’appareil.

### Responsabilités

* L’employé est seul responsable de l’accès mobile qui lui est mis à disposition par l’employeur et de son équipement personnel. L’employeur ne pourra être tenu pour responsable de tout dommage personnel occasionné (matériel, logiciel, perte de données).

### Devoirs

Les employés qui ont un accès de type BYOD s’engagent :

* à ne pas modifier le système d’exploitation de leur appareil (e.g. pas de jailbreak, etc.)
* à ne pas changer, partager ou remplacer la configuration spécifique de l’appareil ;
* ne pas communiquer l’accès à une tierce personne :
* supprimer toutes les données présentes sur l’appareil lors de la clôture de l’accès BYOD.

## Utilisation des ordinateurs de bureau

Les employés qui ont à leur disposition un ordinateur de bureau s'engagent à :

* protéger l'accès à l'ordinateur par un mot de passe répondant aux exigences décrites précédemment ;
* bloquer l'accès à l'ordinateur avant de quitter le poste de travail, même pour un très court laps de temps ;
* prendre toutes les mesures appropriées pour assurer la sécurité des informations stockées sur l’ordinateur ;
* ne pas laisser l’ordinateur à des personnes tierces, excepté aux personnes du service informatique pour des opérations de maintenance ;
* ne pas installer de logiciel sans autorisation du supérieur hiérarchique, sauf ceux autorisés ;
* gérer l'ordinateur en bon père de famille ;
* protéger toutes informations stockées sur un disque local. Lorsqu’il existe un disque réseau les données stockées directement sur la machine sont sous la responsabilité de l’utilisateur. Il est notamment garant de la confidentialité, de l’intégrité et de la disponibilité de l’information stockée en locale ;
* étiqueter explicitement avec la mention « privé », les données privées stockées en local.

## Utilisation d'un Laptop ou d'un Smartphone

### Règles communes d’un Laptop ou d'un Smartphone

Toutes les consignes valables pour les ordinateurs de bureau sont à respecter pour les Laptops et les Smartphones. De plus, le caractère nomade de ceux-ci requiert une attention toute particulière de l’employé qui en a la responsabilité.

Dans le cas d'une attribution permanente ou temporaire d'un appareil, les employés concernés s’engagent à :

* respecter les mêmes consignes que celles des ordinateurs de bureau (chapitre précédent) ;
* prendre toutes les mesures appropriées pour assurer la sécurité physique des appareils portables mis à disposition, notamment de prévenir tout vol ou dommage physique ;
* ne pas se connecter à des réseaux informatiques dont le niveau de confiance est inconnu ;
* effectuer des sauvegardes, lorsqu’il stocke des données sur son appareil portable ;
* veiller à ce que personne ne puisse voir d'informations confidentielles, lorsque l'appareil est utilisé dans un lieu public ;
* ne pas utiliser de WiFi privé au sein de la société ;
* désactiver les moyens de communication sans fil (Wifi ou Bluetooth), y compris la recherche automatique de périphérique, lorsqu’ils ne sont pas utilisés ;
* utiliser le mode de sécurité Bluetooth qui chiffre le trafic dans les deux directions.

### Règles spécifiques aux Laptops

En plus des règles citées ci-dessus, les employés qui utilisent des Laptops s'engagent à :

* utiliser un câble antivol, s'il est indispensable de laisser le Laptop sans surveillance dans des endroits publics ;
* prendre le Laptop comme bagage à main lors des voyages ;
* utiliser un compte utilisateur spécifique disposant de droits restreints, pour accéder à Internet via son Laptop dans les lieux publics tels que les hôtels, les gares, les aérogares, etc. ;
* ne pas entraver le fonctionnement de l'antivirus et du pare-feu, et vérifier qu'ils sont activés et régulièrement mis à jour.

Les Laptops sont attribués aux personnes qui, de par leurs attributions, sont amenées à voyager ou à participer à des foires ou des séminaires au Luxembourg comme à l'étranger.

### Règles spécifiques aux Smartphone

En plus des règles citées ci-dessus, les employés qui utilisent des Smartphone s'engagent à :

* connaître les risques principaux liés aux Smartphone, qui sont en l’occurrence, la perte, la divulgation ou la destruction d’information qui sont généralement facilitées par la taille réduite de l'appareil ;
* protéger l'accès au Smartphone par un code PIN personnel ;
* mettre à jour avec les nouvelles versions de logiciels, dès qu'elles sont disponibles.

Les Smartphones sont attribués aux personnes qui, de par leurs attributions, sont amenées à voyager ou à participer à des foires ou des séminaires au Luxembourg comme à l'étranger.

## Installation de logiciel

Il est interdit de télécharger ou d’installer soi-même des logiciels non autorisés par le service informatique.

## Utilisation de l'accès à distance de la société

Les employés et les tiers autorisés à utiliser l'accès distant de la société ont à leur charge de contracter les services d'un fournisseur d'accès Internet et de supporter les frais associés.

De plus :

* ils ont la responsabilité de s'assurer que des utilisateurs non autorisés ne peuvent pas utiliser leurs droits ou leur infrastructure personnelle pour se connecter au réseau de la société ;
* lorsqu'une connexion à la société est établie, l'utilisateur ne doit en aucun cas, établir d'autres connexions avec d'autres sites distants, ceci pour éviter que l'ordinateur de l'utilisateur ne serve de pont pour les logiciels malveillants ;
* l'ordinateur utilisé pour se connecter à la DMZ, doit disposer d’un antivirus régulièrement mis à jour ;
* en utilisant l'accès distant de la société, l'utilisateur doit comprendre que son ordinateur est un prolongement du réseau de la société. Il est donc sujet aux mêmes règles et règlements qui s'appliquent aux équipements de la société. L'ordinateur doit être conforme à la politique de sécurité de la société ;
* dans le cas de télétravail par exemple, l’employé doit s'assurer qu’aucune tierce personne n’accède aux biens de la société via son accès distant, qu’il n'exerce aucune activité illégale, et n'emploie pas l'accès pour des intérêts commerciaux ou autres. L'utilisateur est responsable des conséquences de tout abus ;
* une connexion inactive pendant 30 minutes est automatiquement fermée. L'utilisateur doit alors rouvrir une nouvelle session. L'utilisation de techniques qui permettent de laisser la connexion ouverte est formellement interdite (ping périodique, etc.) ;
* toutes les connexions d'accès à distance ont une durée de connexion limitée à 24 heures. Au-delà, l'utilisateur doit alors rouvrir une nouvelle session ;
* Les programmes utilisés pour gérer la communication distante ne peuvent être que ceux qui ont été approuvés par le service informatique de la société.

# Usage des services Internet (Web)

L’usage d’internet doit se faire en respectant les règles suivantes :

* l'utilisation d'internet et les accès aux sites doivent être faits dans le respect des règles d'usage propres aux divers sites et réseaux utilisés, et dans le respect de la législation en vigueur.
* l’utilisateur portera une attention particulière au « phishing ». Il veillera qu’il est bien sur le site qu’il souhaite et non sur une contrefaçon. Lorsqu’il saisit des informations sensibles, il s’assurera que la connexion est sécurisée, notamment par la présence d’un cadenas sur son navigateur et que l’URL de la page commence par HTTPS ;
* Il est interdit à tout utilisateurs de surfer sur des sites à caractères insultants, racistes, pornographiques, pédophiles, diffamatoires, violents, ou qui nuiraient à autrui ;
* l’utilisation d’internet à des fins privées est tolérée, cependant elle doit respecter les conditions énoncées ci-dessus et ne doit occasionner aucun trouble ou dysfonctionnement du travail des autres utilisateurs ;
* Le téléchargement à des fins privés, ou qui pourraient nuire au système d’information est interdit. En cas de doute il faut s’abstenir.

# Gestion des emails

## Création d'un compte

Pour les employés qui possèdent une adresse email propre à la société, les comptes sont créés lors de la prise de fonction de l’employé ou lorsqu'un consultant externe intervient pour une mission de durée significative qui en nécessite une.

La dénomination d'un email est le suivant: [Prénom… .Nom @ …](mailto:Prénom.Nom@eco.etat.lu)

L'installation initiale est faite par le service informatique sur le poste de travail de l’employé.

L’accès aux emails est contrôlé par un nom d'utilisateur et un mot de passe répondant aux exigences décrites précédemment.

## Utilisation du courrier électronique

Le système de traitement de courrier électronique de la société est principalement réservé à l’utilisation professionnelle.

Conformément à la loi, chaque employé de la société a un droit à la vie privée au travail. L’usage d’emails pour des raisons personnelles est donc toléré en quantité raisonnable, pourvu que son utilisation n’entrave pas la bonne exécution des tâches quotidiennes de l’employé et de la société. Tout courrier privé doit faire apparaître la mention « privé » dans son objet.

Les courriers électroniques, tout comme les courriers traditionnels, sont soumis à des règles de bienséance :

* il est généralement considéré comme poli de commencer par une formule de salutation, et également d'indiquer un sujet. Il en est de même pour la formule de politesse ;
* l'envoi de pièces jointes est également soumis à des règles de bon sens (poids de l'email en fonction du correspondant) ;
* au cas où un utilisateur recevrait un email qui ressemble à du spam ou à un hoax (c'est-à-dire de l'information non vérifiée et souvent retransmise par des personnes de bonne volonté), il réfléchit et valide lui-même ces informations avant de les accepter et de les transmettre éventuellement à d'autres personnes. Il existe des sites ([www.hoaxbuster.com](http://www.hoaxbuster.com) ou [www.urbanlegends.com](http://www.urbanlegends.com)) permettant de vérifier la véracité du contenu de ce genre d'email. Dans le doute, il est de coutume de ne pas transmettre ce genre de contenu à ses connaissances ;
* l’utilisateur ne doit pas cliquer sur des liens contenus dans les mails sans avoir au préalable vérifier que la source est de confiance.
* l'utilisation de la copie cachée (Bcc, Cci) qui permet d'envoyer un email sans afficher certains destinataires n'est pas autorisée dans l’organisme. Une exception existe, dans le cas d'un envoi de courrier électronique avec votre nom dans « envoyer à : » et tous les autres destinataires en « Bcc, Cci ». D'une façon générale, tous les destinataires doivent être en « Bcc, Cci » ou bien aucun.
* l'écriture en CAPITALES est considérée comme une parole criée, il faut donc éviter de l'utiliser ;
* avant d’intégrer des personnes supplémentaires dans des « discussions » par courrier électronique, demandez l’accord de vos correspondants ;
* éviter d’insérer des animations non utiles dans les courriers électroniques ;
* pour des raisons de sécurité, donner une préférence, si possible, aux messages en format TEXT et non au format HTML.

## Prérogatives à l’envoi d’email

Le courrier électronique est un moyen de communication non sûr (canal de communication public), que ce soit du point de vue confidentialité, intégrité ou disponibilité.

Les employés doivent, avant d’envoyer des informations par courrier électronique, vérifier si le caractère confidentiel de l’information. Seules les données du type publiques peuvent être envoyées en clair. Les données internes, restreintes et confidentielles doivent être chiffrées avant d’être envoyées.

## Sauvegarde des emails

Le système de courrier électronique est un outil de travail et de communication important qui transmet et stocke des informations, à ce titre, le système est sujet à des sauvegardes. Tous les courriers électroniques se trouvant dans les comptes des utilisateurs, sont sauvegardés sans distinction d’un éventuel caractère personnel du courrier électronique.

## Effacement des emails volumineux non professionnels

Afin de garantir la disponibilité des services de courrier électronique, les employés du service informatique vérifient à intervalles réguliers l’évolution de l’espace de stockage restant. Lorsque la disponibilité du service email est menacée par une utilisation excessive des ressources, les employés du service informatique procèdent à une recherche des causes. Selon les cas, ils peuvent prendre des mesures correctives suivant la procédure décrite ci-dessous.

Procédure d'effacement des fichiers personnels volumineux ou gênant :

1. Les employés du service informatique demandent par écrit à ce que les fichiers volumineux personnels soient déplacés ou détruits.
2. Si aucune suite n'est donnée à cette demande, le service informatique peut procéder à l’effacement de ces courriers électroniques.

## Utilisation défendue des emails

Toute utilisation inappropriée qui peut mettre en péril la sécurité du système de courriers électroniques ou qui peut engendrer des préjudices pour la société est défendue.

Il est notamment interdit d’envoyer des courriers électroniques qui ont des contenus répressibles par la loi luxembourgeoise. On peut citer notamment :

* l’abus de confiance (articles 491 à 493 du Code pénal) ;
* l’escroquerie (article 496 du CP) ;
* calomnies, diffamations et injures (articles 443 et suivants ; 448 et 561-7 du CP) ;
* racisme, révisionnisme et discriminations (article 454 du CP) ;
* distribution de pornographie à des mineurs de moins de 16 ans (article 385bis du CP) ;
* pédopornographie (article 384 du CP) ;
* l’envoi d’objets protégés par des droits d’auteurs et droits voisins de tiers ;
* l’envoi de secrets professionnels ;
* l’envoi de documents dont la classification interdit toute transmission par courrier électronique ;
* le spam ou l'envoi, à l’extérieur comme à l’intérieur de la société, de lettres à chaînes ou d’email de plaisanteries.

Les employés recevant de la part d’autres employés de la société, des emails ayant des contenus défendus sont priés d’en avertir le plus rapidement possible leur supérieur hiérarchique, ou le service IT, puisque l'image de la société est mise en jeu.

## Utilisation de la signature électronique

Seuls les employés disposant d’une carte de signature électronique professionnelle (liée avec une adresse propre de la société) peuvent l’utiliser pour les courriers électroniques. Cependant, tous les employés doivent se tenir aux procédures en vigueur pour les mandats de signature et les délégations.

## Utilisation du chiffrement

Si l'utilisation du chiffrement pour protéger la confidentialité d'un contenu est requise, il doit s'effectuer avec les outils cryptographiques validés par la société.

## Sécurité et événements de sécurité

Tous les emails émis ou reçu par un employé de la société passent par une détection antivirus et antispam, en cas de doutes toute personne qui reçoit des courriers électroniques avec des fichiers liés et qui a des incertitudes sur le caractère bénin de ces fichiers (virus par exemple) doit demander au service informatique de vérifier les fichiers en question.

Pour information, il existe un blocage concernant certaines extensions pour les fichiers joints (\*.EXE, \*.RAR, \*.ZIP, etc.).

## Décharge et signature

L'utilisation de la signature électronique est réservée aux employés possédant un droit de signature administrative.

Chaque courrier électronique doit posséder un pied de page standard comportant :

* le nom et prénom de la personne ;
* les coordonnées professionnelles ;

la décharge standard fournie par le service informatique

# Gestion des clés et des badges

Les clés et les badges doivent être comme les mots de passes, c’est-à-dire personnel. Il est donc formellement interdit de prêter sa clé ou son badge à une autre personne. En cas de perte d’un de ces éléments il faut en aviser la personne en charge de la gestion des accès physique.

# Bureau propre

Les papiers et supports informatiques amovibles contenant des informations sensibles ne doivent pas être laissés sans surveillance sur les bureaux. Spécifiquement, les papiers doivent être retirés rapidement des imprimantes, télécopieurs ou photocopieurs, et ne doivent pas être jetés dans les poubelles.

# Mise au rebut

Tout équipement qui est mis au rebut ou réutilisé dans un autre contexte doit être vidé de toutes ses données de façon adaptée à la sensibilité des informations qui s’y trouvent.

Les documents sensibles sont déchiquetés ou déposés dans un conteneur sécurisé.