

GDF SUEZ

ETHIQUE DE LA GESTION
DE L'INFORMATION

CODE DE BONNE CONDUITE

AVERTISSEMENT

Les collaborateurs du Groupe sont tenus d'observer en toutes circonstances les réglementations locales, nationales, fédérales, internationales en vigueur là où ils exercent leurs activités professionnelles.

Lorsqu'un collaborateur envisage de modifier certaines règles exposées dans le présent texte afin d'être conforme à une autre réglementation particulière, d'un niveau plus élevé que celle du Groupe, il doit en aviser le Déontologue de la Branche à laquelle appartient son entité ; le Déontologue de Branche accuse réception et rapporte annuellement sur ces modifications.

Lorsqu'un collaborateur envisage de modifier une règle (ou d'en atténuer sa portée) pour d'autres raisons, il ne peut le faire qu'après avoir reçu l'accord du Déontologue de la Branche à laquelle appartient son entité. Les modifications doivent être dûment motivées et rester conformes à l'esprit du présent texte ; le Déontologue de Branche rapporte annuellement sur les modifications qu'il a autorisées.

Par ailleurs, toute personne travaillant sur les composantes des Systèmes d'Information se rapportant aux données personnelles doit faire preuve d'une éthique toute particulière notamment en matière de confidentialité quant aux données auxquelles elle a accès.

Introduction

LA VIGILANCE, UNE SECONDE NATURE

Les informations que nous manipulons dans notre travail quotidien font partie du patrimoine du Groupe, elles constituent une de ses richesses les plus en vue. Infiniment précieuses, elles sont l'objet de toutes les convoitises. Elles peuvent être copiées, piratées par la concurrence, divulguées (volontairement ou non), manipulées... Leur détournement peut avoir des répercussions graves pour l'entreprise.

“Aussi, est-il du devoir de CHACUN DE NOUS de les protéger en permanence. Cette attention de chaque instant, nous l'avons baptisée “principe de vigilance”, car c'est l'état d'esprit qui doit guider nos actes, du plus anodin au plus sensible”.

Gérard Mestrallet

La vigilance en matière d'information doit devenir notre seconde nature. Efforçons-nous d'en acquérir les réflexes et, avant toute chose, ayons un comportement responsable*.

Vous trouverez dans les pages qui suivent les principes, attitudes et procédures internes permettant un bon usage des informations de l'entreprise.

* les termes suivis d'un astérisque sont commentés dans le “Vade-mecum” en annexe.

ETHIQUE DE L'INFORMATION* : PRINCIPES GÉNÉRAUX

En matière de sécurité de l'information, les équipements, les matériels, les logiciels n'apportent jamais un niveau de prévention absolu mais il faut généralement chercher dans le comportement des individus (malveillance, négligence...) les raisons d'une défaillance. C'est pourquoi un comportement responsable exige de maîtriser les réflexes de base (voir page suivante) mais aussi de faire appel à notre bon sens et à notre savoir-faire dès que nous utilisons des moyens d'information (ordinateurs*, téléphones, documents, etc.). Par exemple, protéger les données professionnelles (confidentielles* ou non) du vol* ne suffit pas, soyons également attentifs à ne pas les divulguer au cours d'une conversation anodine, d'un chat*, dans un blog*, ou même sur un site Web* et en dehors de notre activité professionnelle.

Il existe des données à caractère illégal, des données* qui ne respectent pas la dignité humaine et plus généralement des données choquantes pour certaines catégories de personnes (atteinte aux convictions philosophiques ou religieuses, blagues racistes...). Leur téléchargement*, envoi, conservation, transfert est strictement prohibé au sein des systèmes d'information du Groupe. La même interdiction s'applique aux documents, programmes et données soumis à droits de propriété intellectuelle* (copyright, marques, licences...).

Il est aussi contraire aux règles du Groupe de chercher à dissimuler volontairement notre identité* ou notre appartenance à notre entreprise afin d'obtenir plus facilement des informations ou, inversement, d'effectuer des opérations privées* sous couvert de notre identité informatique professionnelle.

Le système de contrôle et de surveillance du Groupe évalue la conformité de nos conduites avec les dispositions locales applicables. Le non-respect des règles énoncées dans ce code de bonne conduite peut donner lieu, en fonction de la gravité, à des actions correctives et/ou des sanctions* proportionnées aux risques qu'elles font courir à l'entreprise.

POUR UN BON USAGE DES INFORMATIONS DE L'ENTREPRISE...

- Tenons-nous informés des obligations réglementaires et des procédures internes et respectons-les.
- Restons prudents et discrets, en tous lieux, en toutes circonstances.
- Gardons sous contrôle le matériel informatique comme les informations.
- Classifions les informations avant de les diffuser et protégeons-les en conséquence.
- Respectons la traçabilité* et l'intégrité* des informations.

- Choisissons des mots de passe* sécurisés et ne les communiquons à personne.
- N'installons pas de matériel ou de logiciel sur les ordinateurs* sans l'accord du Support Utilisateurs.
- Méfions-nous des virus*, vers* et autres logiciels malveillants.
- Signalons les incidents et les menaces potentielles au Support Utilisateurs.
- En résumé, adoptons en permanence un "comportement responsable".

ATTITUDES ET BONNES PRATIQUES AU QUOTIDIEN

Tenons-nous informés des obligations réglementaires et des procédures internes et respectons-les.

L'usage des technologies de l'information est soumis à des règles issues de lois et de réglementations externes à l'entreprise. Elles visent au respect des intérêts des tiers, par exemple, assurer la confidentialité* des données à caractère personnel ou garantir les droits de propriété intellectuelle*. Elles proviennent également de procédures internes destinées à protéger les intérêts de l'entreprise : protéger les données sensibles, commerciales ou financières, par exemple.

Nous sommes en première ligne en tant qu'utilisateurs des systèmes* d'information de l'entreprise. Pour éviter de porter préjudice* à des tiers ou à notre entreprise – avec toutes les conséquences que cela entraîne à titre personnel ou professionnel – tenons-nous informés des obligations réglementaires et mettons-les constamment en pratique en utilisant l'ensemble des moyens dédiés par le Groupe.

Au bureau, comme à l'extérieur, restons prudents et discrets...

– Dans les lieux publics (train, avion, restaurant...) évitons les conversations professionnelles, téléphoniques ou non, et l'usage de l'ordinateur portable*.

Par principe, ne mentionnons pas notre appartenance à l'entreprise.

– Les réunions, les conversations téléphoniques, les vidéoconférences* doivent se tenir loin des oreilles indiscrettes.

Les conférences téléphoniques et leurs participants doivent, autant que possible, être identifiés par un code d'accès, préalablement diffusé aux seuls participants.

– Les sites Web "sociaux" (myspace, meetic, facebook...) et les forums* de discussion sont fréquemment exploités pour l'espionnage* des entreprises. Évitons d'y citer des faits, des personnes ou des dossiers concernant notre vie professionnelle.

– Nous devons connaître les actions des visiteurs de l'entreprise : ne les laissons jamais seuls dans un bureau ou un espace de travail. Accueillons-les et raccompagnons-les à la sortie des bâtiments.

- Restons sur nos gardes avec les personnes qui nous questionnent sur l'entreprise. Si une personne (connue ou non) nous approche pour obtenir des informations confidentielles* sur le Groupe ou une de ses entités, abstenons-nous de les lui fournir. Si cette personne insiste, informons notre supérieur hiérarchique, le déontologue ou le responsable de la sûreté, s'il y en a un dans l'entité.
- Avant de répondre à une enquête téléphonique, assurons-nous de la destination et de la protection des informations divulguées. En cas de doute, ne répondons pas.
- Ne donnons à nos interlocuteurs (internes ou externes) que les renseignements qu'ils peuvent ou doivent légitimement connaître et dont ils ont réellement besoin. N'oublions pas de leur indiquer le niveau de confidentialité* des informations délivrées (voir Classification des informations).
- Ne prêtons jamais ni portable*, ni clés* USB personnels à qui que ce soit. N'autorisons pas la connexion de clés USB qui ne seraient pas fournies par le Service Informatique d'une entité du Groupe.
- Lors des déplacements, n'emportons que les informations (documents, clés USB) strictement indispensables.

Gardons sous contrôle le matériel informatique comme les informations.

Les vols* de documents papier ou de dossiers sont aussi graves que les vols de matériel. Il est essentiel de protéger du vol aussi bien les supports d'information que les informations qu'ils contiennent.

Veillons sur le matériel :

- Le matériel informatique et de communication que fournit l'entreprise est sous notre responsabilité personnelle. Rangeons-le dans un endroit sécurisé dès que nous nous absentons du bureau et ne le laissons en aucun cas sans surveillance (salle de réunion, véhicule, train, lieu public...)
- Il existe un autre moyen de protéger les ordinateurs portables* contre le vol : utiliser un câble de sécurité verrouillé.

Veillons sur les données :

- Prenons garde de ne rien égarer. Par exemple, à la fin d'une réunion, quand les participants ont quitté la salle, vérifions qu'il ne reste aucun document ni matériel sur les tables, aucune information inscrite au tableau. Avant de quitter le bureau le soir, rangeons tous les documents et/ou assurons-nous qu'ils sont en sécurité.
- Ne laissons pas des documents sensibles visibles dans un véhicule ou sur un siège dans le train ou dans un lieu public.
- Il est important de ne conserver qu'un seul exemplaire des documents classés "Strictement Confidentiel*". Lorsqu'ils sont périmés (selon les critères réglementaires), détruisons-les, de préférence en utilisant la déchiqueteuse.
- Retirons au plus vite des imprimantes*, fax* ou photocopieuses* partagées les documents imprimés dont le contenu est "Strictement Confidentiel" ou à "Diffusion restreinte". Les indiscretions et les vols de documents sont fréquents à cet endroit.
- Avant de faxer des documents confidentiels, appelons le destinataire pour

le prévenir, contrôlons le numéro avec lui et demandons-lui un accusé de réception. – Il est préférable d’envoyer (et de demander) par courrier les exemplaires originaux de documents légalement contraignants.

Classifions les informations avant de les diffuser et protégeons-les en conséquence

A : La classification*

Un grand nombre d’informations détenues par l’entreprise ne doivent pas être communiquées à l’extérieur et sont parfois même adressées seulement à un petit nombre de collaborateurs. Classifier des informations consiste en une évaluation et une indication claire de leur degré de confidentialité à observer, à la fois personnellement et par les collaborateurs. Le propriétaire⁽¹⁾ d’un document (généralement son auteur) doit indiquer sa classification parmi quatre niveaux possibles :

1/ “Strictement Confidentiel” – informations susceptibles de présenter, en cas de divulgation, des répercussions graves pour l’entreprise. Leur consultation, copie et diffusion ne sont autorisées que moyennant autorisation explicite de leur propriétaire. Celui-ci tient une liste de l’ensemble des personnes ayant consulté ou traité ces données.

2/ “Diffusion Restreinte” – informations susceptibles, en cas de divulgation, d’un impact substantiel sur les intérêts de l’entreprise. L’accès est limité à un groupe de personnes précis, parfois externes à

l'entreprise, dont la liste est répertoriée sur le document support.

3/ "Usage Interne" de l'entreprise – informations internes dont la publication présenterait un impact limité à l'extérieur de l'entreprise, mais pouvant toutefois avoir des conséquences pour certaines personnes.

4/ "Public" – informations destinées au grand public.

Si un document est non classifié, il est considéré à "Usage Interne" par défaut, sauf dans le cas où une réglementation en décide autrement (ex. : certains documents contenant des données à caractère personnel ou, dans certains pays, les documents émanant de juristes qui ont un statut "privilegié", ces documents sont donc "strictement confidentiels", par défaut).

⁽¹⁾ *Important* : seul le propriétaire d'un document (l'auteur) peut en modifier* la classification.

B : La protection

Le vol* d'informations ne concerne pas uniquement les PC. La consultation ou l'écoute illicite d'informations confidentielles* (via téléphone mobile, pda*, smartphone*, pocket pc, sur imprimantes*, fax*, dans les archives et les dossiers...) est très fréquente et cause des préjudices* à nombre d'entreprises. Veillons à limiter les risques :

– Sauvegardons* les informations confidentielles sur le serveur*, et non sur les disques locaux.

- Lorsqu'ils sont sans surveillance, (même pendant un court instant) les documents, supports d'informations (disques, DVD, CD-ROM, clés USB* ...) doivent être enfermés sous clé et les PC verrouillés* . Le Support Utilisateurs peut nous indiquer les moyens d'un verrouillage automatique après quelques minutes d'inaction.
- Mettons à jour régulièrement, notamment lors du départ, changement d'affectation ou mutation* d'un collaborateur, la liste des utilisateurs ayant accès sur le serveur aux répertoires dont nous sommes titulaires.
- Transmettre une information confidentielle* par tout courrier électronique* dans les boîtes e-mail personnelles comporte des risques importants de piratage* . Échangeons, de préférence, les informations professionnelles à travers les dossiers partagés et les bases de données du système d'information de l'entreprise. Si toutefois une transmission par courrier électronique doit avoir lieu, utilisons si possible l'encryptage* , ou, à défaut, d'autres moyens de protections (ex. : fichier ZIP* avec mot de passe).
- Tous les courriers électroniques* envoyés vers l'extérieur par les entités du Groupe doivent comporter une mention finale indiquant leur caractère confidentiel et, le cas échéant, la protection légale de cette confidentialité (ex. : courriers électroniques rédigés par des consultants juridiques, dans certains pays). La mise en œuvre de cette mention doit être effectuée par le management de l'entité.
- Lorsqu'un document sensible, sur lequel de nombreux ajouts ou corrections ont été apportés, doit être envoyé, il est indispensable d'empêcher

le destinataire d'effectuer une recherche de ces modifications* successives (appelée "recherche de métadatas*" ou "reverse engineering" du document). Le Support utilisateurs ou informatique peut, à la demande, nous en fournir les moyens.

- Évitions de traiter des informations concernant notre activité professionnelle sur un ordinateur connecté sur d'autres réseaux que celui d'une entreprise du Groupe (notamment, les ordinateurs familiaux, car ils peuvent être insuffisamment protégés).
- En fin de vie, restituons le matériel informatique au Département Informatique qui effectuera son reconditionnement (destruction de certaines informations) ou sa destruction physique en fonction des impératifs de sécurité.

Respectons la traçabilité* et l'intégrité* des informations

La connaissance de la source d'une information est une donnée importante. Indiquer ses sources et respecter l'intégrité d'un texte d'origine est une règle essentielle, elle diminue le risque de plagiat ou de faux ou de contrefaçon. Supprimer ou altérer de l'information, par exemple, afin de faire disparaître des preuves ou déformer des faits est strictement interdit et entraîne de lourdes sanctions pour leurs auteurs. Ainsi, lors du transfert ("forward") d'un courrier électronique*, le texte ne doit en aucun cas être modifié*.

Conserver trace des informations et des destinataires des données dont nous sommes ou avons été détenteur

est un moyen de preuve qui s'avère utile en cas de problème ou de contestation. Les systèmes d'information prennent parfaitement en compte cette traçabilité. Ainsi, la consultation d'un site Web* ou l'envoi d'un courrier électronique*, laisse toujours une trace dans l'ordinateur* et/ou sur les serveurs*. La méconnaissance de cette caractéristique permet, par exemple à la police, de retrouver les individus consultant les sites interdits (pédophilie*, pornographie*, terrorisme...) malgré leurs vaines précautions (pseudonymes, trucages de photos, suppression de données dans leur PC...).

Choisissons des mots de passe* sécurisés et ne les communiquons à personne.

Chaque mot de passe (identifiant, login) constitue un élément clé de la sécurité du système d'information du Groupe. Cette sécurité est réduite à zéro dès qu'un mot de passe est écrit ou conservé négligemment sur un écran d'ordinateur, un bureau, sous un tapis de souris, un clavier ou même dans un tiroir non fermé à clé. Idéalement, mes mots de passe ne devraient être stockés qu'en un seul endroit : notre mémoire.

– Les mots de passe constitués de dates d'anniversaire, noms de personnes, numéros de téléphone ou de mots du dictionnaire – mêmes épelés à l'envers – sont faciles à “casser” pour les spécialistes en informatique. N'utilisons que des mots de passe sécurisés ; c'est-à-dire, composés au minimum de huit signes et d'un mélange de majuscules, de

minuscules, de chiffres et de caractères spéciaux tels que : “ ! & @ # \$ % ^ `? ...

– Les mots de passe sécurisés ne se communiquent à personne.

Si, par inadvertance, ou, par exemple, à l’occasion d’une opération de maintenance, ils ont été dévoilés, il est indispensable de les changer sans tarder. Si nous soupçonnons quelqu’un de connaître un mot de passe, il faut également le modifier. De même, il est indispensable de changer les mots de passe qui sont attribués automatiquement, en tant que “nouvel utilisateur”.

– N’employons jamais, sur des réseaux externes, d’autres serveurs*, ou sur des sites Internet, un nom d’utilisateur (et/ou un mot de passe) déjà utilisé au sein de l’entreprise.

N’installons jamais de matériel ou de logiciel sur nos ordinateurs* sans l’accord du Support utilisateurs.

Même d’apparence anodine, toute adjonction de matériel ou de logiciel doit être précédée d’une étude du “Support Utilisateur”.

En effet, les risques sont grands : ainsi, un modem installé sans autorisation peut accroître le risque de fuite d’informations dans l’ensemble du réseau. Un logiciel non homologué peut comporter des virus*, générer des failles de sécurité, être en infraction vis-à-vis de la propriété intellectuelle* ou du droit d’usage. Pour toutes ces raisons, l’installation des matériels ou des logiciels, même gratuits, sans l’accord du Support Utilisateurs est interdite.

Méfions-nous des virus* , vers* et autres logiciels malveillants

Les virus informatiques (également appelés “malwares*”) sont des programmes conçus dans le but de nuire, d'endommager gravement les fichiers, les programmes voire même tout le réseau de l'entreprise.

– La première prévention consiste à ne jamais ouvrir les pièces jointes des courriers électroniques* émanant d'un émetteur non-identifié ou inconnu. Mais ce n'est pas une garantie absolue : beaucoup de virus se propagent via les carnets d'adresses et peuvent donc nous parvenir par nos correspondants habituels, ils peuvent également provenir de supports amovibles non vérifiés par le Support informatique.

– Ne cherchons pas à analyser les problèmes (virus, intrusion), car la manipulation pourrait détruire certaines preuves essentielles. Si nous soupçonnons notre PC d'être infecté : déconnectons-le du réseau afin d'éviter toute propagation de l'infection, mais attention, ne l'éteignons pas, afin de faciliter les investigations ultérieures. D'une façon générale, informons immédiatement le Support Utilisateurs.

– N'essayons jamais de “tester” la protection d'un système ou d'une application au risque d'être accusé d'intrusion.

Signalons les incidents et les menaces (même potentielles)

Tout incident* ou menace relatif à la sécurité de l'information peut avoir des conséquences graves pour l'entreprise. Signalons sans tarder au supérieur hiérarchique, au Support Utilisateurs, au déontologue, ou mieux, au Responsable de la Sûreté s'il y en a un dans l'entité :

- un manque de protection quel qu'il soit (ex : serrure défectueuse, mauvaise classification) ;
- un incident, si minime soit-il (ex. : perte de clé, comportement étrange d'un visiteur, disparition d'objets...) ;
- toute dégradation, perte ou vol* du matériel de l'entreprise (PC, fixe ou portable*, imprimante*, clé USB*, smartphone ou tout autre équipement informatique) ;
- des failles (avérées ou même supposées) dans le système de sécurité.

Adoptons en permanence un comportement responsable*

A tout moment les informations professionnelles doivent être protégées, voilà notre objectif personnel. Aucune organisation ne peut fonctionner correctement avec des gens irresponsables ; il suffit d'un seul maillon faible pour que la chaîne de la sécurité se brise. Vouloir assumer ses responsabilités en toutes circonstances est à la fois une décision de prudence et de sagesse. Quand le bon sens gouverne nos actions, la majeure partie des risques existants en matière de sécurité est sous contrôle (jamais la totalité !).

Il est donc de notre devoir de :

- rester vigilant en permanence (dans l'entreprise, en déplacement, à la maison) ;
- suivre les conseils des techniciens du support utilisateur ou informatique ;
- et enfin, de participer aux formations qui sont proposées par l'entreprise pour maîtriser les risques.

CONTRÔLE, SURVEILLANCE ET SANCTIONS*

Le Groupe possède dans chaque entreprise un dispositif de contrôle et de surveillance. Conformément aux règles exposées dans ce document et aux dispositions locales prises en application dans le cadre des lois applicables, ce dispositif est destiné à veiller au respect de la protection des intérêts économiques du Groupe au moyen d'une utilisation responsable des systèmes d'information et du maintien de leur sécurité. La DSI, la DRH, l'Audit ou les Services de Sécurité concernés localement ont un rôle particulier à assumer pour veiller à ce respect.

En tant qu'utilisateur, nous possédons une grande autonomie dans l'usage des systèmes d'information. Ceci nous confère en retour des responsabilités étendues sur l'usage de ces systèmes. Le premier contrôle est donc celui que nous assurons pour notre propre compte, sur la base des présents principes.

Les dysfonctionnements observés peuvent, le cas échéant, donner lieu à des actions de correction, mais aussi à des sanctions,

proportionnées aux risques qu'ils font courir à l'entreprise. Ces sanctions peuvent prendre la forme de sanctions disciplinaires ainsi que judiciaires et, dans les cas les plus graves, entraîner le licenciement d'un membre du personnel ou la rupture du contrat d'un prestataire. Toute mesure prise sera conforme aux dispositions légales, notamment de Droit Social, ou, le cas échéant, celles relatives à la protection de la vie privée*, en vigueur localement.

Important : les principes contenus dans ce document sont applicables tant aux membres du personnel qu'aux prestataires externes qui devront être tenus informés de leur application.

VADE-MECUM

ETHIQUE DE LA GESTION DE L'INFORMATION

Introduction

En complément du “Code de bonne conduite”, vous trouverez dans les pages qui suivent, par ordre alphabétique, les notions importantes : définition, risques encourus et les moyens de s'en protéger.

Mode d'emploi

Pour chaque terme, vous trouverez les rubriques suivantes :

- 1** - Définition ou responsabilité
(compliance, préjudices et sanctions)
- 2** - Risques
- 3** - Protection de l'information
- 4** - Protection de l'identité
- 5** - Protection du matériel / processus
- 6** - Consigne

Edition mai 2008

Une version électronique est disponible sur
<http://ethics.suez.com> (mot de passe : ethics)
<http://smile.group.suez>

Adresse IP

- Un numéro d'identification est toujours attribué à un ordinateur ou un autre matériel qui se connecte sur l'Internet. Ce numéro permet notamment de savoir à quel réseau appartient ce matériel.

- **Risques** : L'usurpation de l'adresse IP afin d'acquérir illicitement des droits d'accès.

En cas d'utilisation illicite de l'ordinateur, l'adresse IP permet son identification.

- **Protection de l'information** : L'adresse IP permet de protéger l'identité de l'utilisateur.

- **Protection de l'identité** : Risque d'usurpation d'identité en cas de prêt ou de vol de l'ordinateur.

- **Protection du matériel / processus** : Ne jamais prêter son ordinateur, le protéger du vol.

- **Consigne** : La DSI doit posséder la liste des adresses IP des ordinateurs appartenant à l'entreprise.

Agenda électronique (PDA, Smartphone)

- Encore appelé organisateur ou ordinateur de poche, l'appareil associe les fonctions téléphonie, navigation Web, agenda, liste de contact, appareil photo, lecteur multimédia, messagerie électronique et utilise les technologies sans fil (exemple : Wi-Fi).

- **Risques** : L'interception des données peut se faire par vol matériel ou par espionnage des réseaux sans fil. Les fabricants de certains matériels prévoient parfois de transmettre automatiquement des données et de surveiller à distance certains paramètres des appareils.

- **Protection de l'information** : Utiliser les dispositifs de verrouillage, code secret et mots de passe. Ne jamais prêter un appareil. Les modes téléphone et messagerie ne garantissent pas un haut niveau de confidentialité. La connexion des matériels sur le réseau de l'entreprise doit être autorisée par la DSI.

- **Protection de l'identité** : Risque d'usurpation d'identité en cas de prêt ou de vol.

- **Protection du matériel** : Appliquez le même type de protection que celui que vous pratiquez pour votre agenda ou portefeuille personnel.

- **Consigne** : Tout utilisateur doit connaître les risques de non-confidentialité, les règles d'usage licite d'Internet ainsi que les conditions de traçabilité des connexions. La DSI doit posséder la liste des personnes autorisées à utiliser ces matériels sur le réseau de l'entreprise.

Alerte professionnelle

Voir "reporting des incidents".

Archivage

- Des réglementations, soit externes, soit internes, imposent de conserver les informations sous forme électronique ou matérielle pendant des durées variables.

- **Risques** : Perte, destruction ou vol de documents, fichiers ou données.

- **Protection de l'information** : Utiliser les dispositifs de verrouillage, codes secrets et mots de passe pour accéder aux archives. Respecter la "classification" (voir ce mot) des archives. Vérifier la confidentialité des échanges. Ne jamais détruire un document archivé sans être informé de sa durée légale de conservation (déterminée par des réglementations et/ou des règles internes).

- **Protection de l'identité** : Risque d'usurpation d'identité pour la consultation frauduleuse des archives classifiées.
- **Protection du matériel / processus** : Les lieux où les données sont archivées doivent être sécurisés vis-à-vis des risques de destruction ou d'intrusion physique ou électronique.
- **Consigne** : Tout utilisateur doit connaître les risques disciplinaires ou judiciaires liés à la destruction volontaire ou non de données.

Authentification

Voir "identifiant".

Autorisation d'utilisation des moyens d'information de l'entreprise

- Sauf exception, une personne ayant accès aux moyens d'information de l'entreprise n'a jamais accès à l'ensemble de ces moyens. La DSI tient à jour les droits d'accès de chaque utilisateur du système d'information de l'entreprise. Les chefs de service définissent pour chacun de leurs collaborateurs les conditions d'accès aux applications, systèmes, équipements, et, plus généralement, aux types d'information qui les concernent.
- **Risques** : Usurpation d'identité, perte de confidentialité.
- **Protection de l'information** : Les informations échangées doivent être limitées à celles qui doivent être connues des destinataires pour des raisons professionnelles. Utiliser les dispositifs de verrouillage, code secret et mots de passe
- **Protection de l'identité** : "Mot de passe" sécurisé (voir ce mot). Les droits d'accès sont personnels, ils ne peuvent être ni cédés, ni détournés, même de façon temporaire. Un collaborateur doit demander à son supérieur hiérarchique d'augmenter ou de restreindre ses droits en fonction de l'évolution de ses besoins.
- **Protection du matériel / processus** : Ne jamais utiliser un équipement (1) sans y être autorisé et (2) sans en connaître le mode d'emploi.
- **Consigne** : Tout utilisateur doit connaître ses droits d'accès. Les propriétaires de l'information conservent la liste des accès autorisés et la mettent à jour régulièrement.

Blog

- Un blog est une sorte de journal personnel tenu sur un site Web. Certaines entreprises tiennent des blogs, par exemple pour la promotion de leurs marques, qui sont alors sous la responsabilité de leur service de la communication.
- **Risques** : Divulgence d'informations confidentielles, rumeurs, diffamation. Transmission de virus, infractions diverses (droits de la propriété intellectuelle, vie privée, concurrence, voire lois sur la presse, droit de réponse...).
- **Protection de l'information** : Un collaborateur doit éviter de livrer des informations relatives à l'entreprise dont il est le salarié (à moins qu'il ne soit habilité à parler en son nom). Il doit également éviter d'agir en contradiction avec d'autres réglementations, notamment quand il utilise un blog personnel dans sa vie privée. Un collaborateur qui rédige un blog doit être prudent, la diffusion d'une rumeur, d'une accusation, d'une fausse nouvelle ou d'une information confidentielle peut avoir des conséquences personnelles et professionnelles catastrophiques. La consultation ou la rédaction d'un blog est rarement justifiée dans le cadre de l'activité professionnelle des collaborateurs du Groupe.
- **Protection de l'identité** : L'auteur d'un blog peut cacher sa véritable identité ou usurper celle d'une autre personne ou institution. En cas de préjudice, les services de police retrouvent généralement assez vite le nom de l'auteur véritable.

- **Protection du matériel / processus** : Pour éviter les virus, n'ouvrez jamais un log d'une personne ou institution que vous ne connaissez pas.
- **Consigne** : Tout collaborateur doit savoir qu'il est déconseillé, sauf justification professionnelle, de consulter, ou de rédiger des blogs pendant le temps de travail. Cette consultation peut être interdite dans certaines entités, vérifiez vos règles locales. Les blogs d'entreprise ou de marque ne peuvent être confiés qu'aux services de la communication, à des collaborateurs spécialement formés et conseillés par des services juridiques internes ou externes (il est conseillé d'écrire une "charte du blog" afin d'en préciser les conditions et usages autorisés).

Bogue (ou bug)

- Un bogue est un défaut de programmation ou de réalisation à l'origine d'une anomalie informatique (voir incident)
- **Risques** : Selon le type de bogue, les conséquences de l'anomalie peuvent être bénignes ou gravissimes (l'explosion en vol de la fusée Ariane V, le 4 juin 1996, suite à une erreur de programmation !).
- **Protection de l'information** : L'utilisateur qui s'aperçoit de l'existence d'un bogue doit en avvertir le support informatique ("support utilisateur", "helpdesk", "service desk"...) sans délai.
- **Protection de l'identité** : Un bogue peut avoir un effet sur l'identification (ex. : difficulté d'authentification, erreur d'adresse...).
- **Protection du matériel / processus** : Un bogue est généralement sans effet grave sur le matériel informatique mais peut avoir des effets sur les applications.
- **Consigne** : Tout utilisateur doit connaître les coordonnées du service de maintenance informatique ("support utilisateur", "helpdesk", "service desk"...) et lui signaler les bogues.

Chat (exemple : MSN, Yahoo Messenger)

- Un chat est une discussion en ligne, entre deux ou plusieurs personnes, qui s'effectue en temps réel (messagerie à transmission instantanée) par écrit ou en vocal. On utilise le verbe "chatter".
- **Risques** : Virus, mais surtout risque d'indiscrétion, de diffamation, de harcèlement, de propos/messages inappropriés, rumeur, perte de confidentialité, non-respect de la vie privée, dissimulation, voire usurpation d'identité. Irresponsabilité liée à l'anonymat, le cas échéant.
- **Protection de l'information** : Il est déconseillé d'utiliser les moyens informatiques de l'entreprise pour "chatter", ceci peut être interdit dans certaines entités du Groupe : vérifiez les règles locales. Dans sa vie privée, un collaborateur doit être prudent sur les informations livrées au cours d'un chat, il est dangereux d'aborder des sujets relatifs à l'entreprise, voire à sa vie professionnelle.
- **Protection de l'identité** : La dissimulation d'identité est fréquente dans les chats, les malfaiteurs utilisent fréquemment ce moyen pour tromper une personne sur leurs réelles intentions.
- **Protection du matériel** : En interdisant la connexion à des sites de chat, l'entreprise diminue le risque de virus et de perte de confidentialité.
- **Consigne** : Tout utilisateur doit connaître l'interdiction de se connecter à des sites de chat avec le matériel de l'entreprise.

Classification de l'information :

• L'information propriété de l'entreprise fait partie de son capital intellectuel, celui-ci ne peut être disséminé sans précautions. La classification consiste à identifier simultanément les personnes et les données qui peuvent être portées à leur connaissance. En pratique, le Groupe distingue quatre niveaux de classification "Strictement Confidentiel", "Diffusion Restreinte", "Usage Interne", "Public". Tout document doit comporter une indication de sa classification (à défaut, il est considéré à "Usage Interne").

• **Risques** : Divulgence d'informations confidentielles, dissémination inappropriée des savoir-faire ou des secrets de fabrication, mise en danger de l'entreprise.

• **Protection de l'information** : Les collaborateurs doivent s'informer sur les règles de la classification en vigueur dans le Groupe.

• **Protection de l'identité** : Quelle que soit sa forme, un document doit permettre d'identifier le responsable (l'auteur, le propriétaire, la source) de ce document.

• **Protection du matériel / processus** : La sécurité des accès aux lieux (physiques ou virtuels) où sont conservés les documents est à la base d'un bon système de protection de leur classification.

• **Consigne** : Tout utilisateur doit savoir classer et connaître le niveau de classification des documents auxquels il a accès et ses conséquences (méthode de classification, règles de transmission des documents, protection/archivage).

Clés USB

• La clé USB est une mémoire externe de petit format connectable sur un port USB d'un ordinateur. Les données peuvent être écrites, modifiées, effacées à la demande.

• **Risques** : Virus, logiciels espions, vol de données.

• **Protection de l'information** : Il est possible grâce à la connexion d'une clé USB de soutirer discrètement les informations stockées dans un ordinateur. Il est également possible d'y transférer des virus ou logiciels espions. Évaluez les risques avant de prêter votre clé USB, pour éviter que son contenu soit volé ou altéré. Ne jamais accepter qu'une personne branche sa clé dans un port de votre ordinateur (à moins que cette clé lui ait été fournie par votre entreprise).

• **Protection de l'identité** : Ne jamais prêter votre clé USB, ne jamais accepter qu'une personne branche sa clé dans le port de votre ordinateur (à moins que cette clé lui ait été fournie par votre entreprise).

• **Protection du matériel** : Toujours tenir les clés USB en lieu sûr (retirer la clé de son port USB lorsque l'utilisateur s'absente, la placer dans sa poche ou un tiroir fermé à clé).

• **Consigne** : Tout collaborateur doit connaître les risques liés aux clés USB, et protéger les siennes du vol.

Code

Voir "encryptage" et "identifiant".

Compliance

• La compliance est un processus qui consiste à prendre les mesures nécessaires pour se mettre en conformité avec une réglementation ou une exigence éthique.

• **Risques** : Les risques de non-compliance sont des sanctions de nature disciplinaire, judiciaire et/ou réputationnelle.

• **Consigne** : Le dispositif de sécurité de l'information du Groupe est un outil de compliance. Les collaborateurs doivent être capables d'identifier les domaines où ils sont concernés par ce dispositif.

Concurrence

- Les échanges d'information entre concurrents sont réglementés par les autorités de la concurrence au niveau national ou international (OCDE, OMC, UE...).
- **Risques** : Distorsion de marché, entente, risque réputationnel, poursuites judiciaires, amendes très élevées.
- **Protection de l'information** : Les collaborateurs doivent être vigilants dans leurs rencontres avec des concurrents et lors de leurs échanges d'information avec eux. Ne jamais échanger sur les prix, les conditions de vente ou d'achat, sans le conseil d'un juriste.
- **Protection de l'identité** : La dissimulation d'identité peut contribuer à commettre une infraction aux règles de la concurrence.
- **Consigne** : Les collaborateurs susceptibles d'être en relation avec des concurrents doivent savoir comment éviter les infractions aux règles de la concurrence.

Confidentialité

- Toute information professionnelle (financière, technique, sociale) créée ou détenue par l'entreprise et/ou ses collaborateurs est considérée a priori comme confidentielle et ne peut être divulguée à l'extérieur de l'entreprise que par des personnes ou services habilités à le faire.
- **Risques** : Perte de secrets et d'avantages compétitifs, escroquerie, atteinte à la vie privée, délits d'initié, chantage.
- **Protection de l'information** : Tout transfert d'informations doit respecter la politique de classification du Groupe (voir "classification de l'information").
- **Protection de l'identité** : La diffusion des données à caractère personnel peut constituer des atteintes à la vie privée et enfreindre certaines réglementations (notamment en Europe).
- **Protection du matériel** : Les lieux réels ou virtuels, où les données confidentielles ou ayant un caractère personnel sont stockées (même temporairement), doivent être sécurisés vis-à-vis des risques de destruction ou d'intrusion physique ou électronique.
- **Consigne** : Tous les collaborateurs susceptibles de détenir des informations confidentielles doivent connaître les règles les concernant. Les supérieurs hiérarchiques vérifient leur respect périodiquement.

Contrôle (audit et surveillance)

- En ce qui concerne le dispositif de sécurité de l'information du Groupe, le contrôle se définit comme le processus d'évaluation de la conformité de la gestion des informations vis-à-vis de critères préétablis. Ce processus fait appel à des méthodes d'observation, d'inspection, d'interrogation, de sondage, d'échantillonnage, de mesure... Les opérations de contrôle sont elles-mêmes soumises à des règles éthiques (confidentialité, vie privée...).
- **Risques** : Le contrôle permet de vérifier que la conformité apporte une réponse pertinente aux risques existants et potentiels.
- **Protection de l'information** : Les rapports d'audit sont confidentiels.
- **Protection de l'identité** : Les contrôles respectent la vie privée des personnes contrôlées. Les rapports sont confidentiels et seules les personnes qui ont des raisons professionnelles pour les connaître ont accès aux informations qui leur sont nécessaires dans l'exercice de leur fonction.
- **Protection du matériel / processus** : Les contrôles des matériels et processus utilisés par les collaborateurs sont nécessaires pour s'assurer de la sécurité du système d'information.

• **Consigne** : L'organisation du contrôle est de la responsabilité de l'audit interne. Cependant, chaque utilisateur exerce un premier niveau de contrôle en s'assurant de bien connaître et appliquer les règles relatives aux équipements dont il dispose et aux process qu'il met en œuvre.

Connexion

• Procédure permettant d'établir un lien entre deux équipements ou systèmes informatiques (exemple : entre un ordinateur et un autre ordinateur, et un serveur, et Intranet...). La procédure d'échange d'informations est souvent précédée d'une phase d'authentification, où l'équipement qui se connecte est identifié avec certitude par l'équipement ou système récepteur.

• **Risques** : Virus. Intrusion (logiciels espions). Certaines connexions sont interdites par la réglementation externe (site illégal) ou interne (site de jeux, sites pornographiques...)

• **Protection de l'information** : Si vous utilisez votre PC en déplacement ou chez vous, utilisez des procédures de connexion sécurisées quand vous vous connectez au réseau de l'entreprise. De même, ne connectez jamais votre ordinateur à des réseaux non sécurisés. Méfiez-vous des réseaux sans fil (exemple : Wi-Fi). Demandez conseil au support informatique ("support utilisateur", "helpdesk", "service desk"...)

• **Protection de l'identité** : Il est prudent de s'assurer de l'identité des personnes/sites qui vous interrogent. Les sites sécurisés se distinguent par le préfixe : <https://> et non pas <http://>. Protégez votre identité en utilisant des "mots de passe" (voir ce mot) sécurisés.

• **Protection du matériel /processus** : Se connecter à des réseaux peu protégés entraîne des risques de virus ou d'intrusion.

• **Consigne** : Les utilisateurs doivent être sensibilisés aux risques liés aux connexions non sécurisées et savoir qu'il est interdit de cacher leur identité (dans le but d'entraver la traçabilité) dans le cadre d'une utilisation professionnelle des systèmes d'information du Groupe.

Courrier électronique

Voir "e-mail".

Cybercriminalité

• Le terme cybercriminalité désigne l'ensemble des infractions pénales commises au moyen de systèmes informatiques : fraude, trafic, vol, escroquerie, harcèlement, diffamation, pédophilie...

• **Risques** : Les risques sont la condamnation pénale et le risque réputationnel.

• **Protection de l'information** : Utiliser un système d'information d'entreprise pour commettre un cybercrime peut entraîner la recherche de la responsabilité pénale de ladite entreprise (co-auteur du crime ou complice).

• **Protection de l'identité** : Un ordinateur possède systématiquement un identifiant (adresse IP). Grâce à cet identifiant, les enquêtes sur les cybercrimes perpétrés à partir des équipements de l'entreprise sont généralement conclues rapidement, même quand leurs auteurs cherchent à dissimuler leur identité (la dissimulation d'identité est une pratique interdite dans le Groupe).

• **Protection du matériel** : Seule la prise de conscience des responsabilités de chacun permet de limiter les vols ou la destruction des matériels et des données.

• **Consigne** : Les collaborateurs doivent savoir qu'un cybercrime les expose à des sanctions pénales et disciplinaires (pouvant aller jusqu'à des peines de prison et au licenciement).

Dénigrement

- Le dénigrement est une action non fondée par laquelle une entreprise tente de jeter le discrédit sur un de ses concurrents. En français, on utilise plutôt le terme “diffamation” (voir ce mot) entre particuliers, tandis qu’entre entreprises on préfère le mot “dénigrement”. Une action de dénigrement peut être considérée comme un acte de concurrence déloyale. Dans de nombreux pays, le dénigrement, comme la diffamation ou l’injure, sont des infractions pénales.

- **Risques** : Risque civil ou pénal (notamment, en cas d’utilisation des systèmes d’information de l’entreprise). Risque réputationnel pour la victime comme pour l’auteur de la diffamation.

- **Protection de l’information** : Les collaborateurs doivent être attentifs à ne pas se rendre coupable de dénigrement. Dans le cas où une entité du Groupe est victime de dénigrement, le collaborateur qui s’en aperçoit doit contacter son supérieur hiérarchique. Les services juridiques du Groupe sont en charge de gérer ces situations.

- **Protection de l’identité** : Il est interdit de dissimuler son identité dans le but de se livrer à des actions de dénigrement.

- **Consigne** : Les collaborateurs doivent être informés sur les risques liés au dénigrement. Ces risques concernent à la fois l’auteur et son entreprise.

Déplacement (déménagement de matériel)

- Les matériels dont sont dotés les collaborateurs peuvent être déplacés pour plusieurs raisons : échange de matériel, nouvelle affectation du matériel, fin de location du matériel, mise au rebut du matériel, déménagement du collaborateur, mutation, fin de mission... Ceci peut entraîner une nouvelle définition des informations à mettre à la disposition (droits d’accès) du détenteur du matériel ou du nouveau détenteur du matériel.

- **Risques** : Perte, vol de données. Perte de confidentialité. Divulgence d’informations personnelles. Droits d’accès non pertinents.

- **Protection de l’information** : En cas de déplacement, les données contenues dans le matériel déplacé doivent être analysées, et les données non pertinentes (en fonction de la nouvelle affectation) doivent être définitivement effacées des mémoires par l’utilisation de méthodes spécifiques (il n’est par exemple pas suffisant d’effacer le contenu d’un disque dur en utilisant les commandes habituelles, car des programmes spéciaux permettent de reconstituer l’ensemble des données).

- **Protection de l’identité** : Les droits d’accès doivent être redéfinis à chaque modification d’affectation du matériel ou de son détenteur.

- **Protection du matériel /processus** : Les matériels et leurs détenteurs doivent être identifiables, car les détenteurs sont responsables de leur matériel.

- **Consigne** : Le service en charge de vérifier les équipements déplacés est le support informatique (“support utilisateur”, “helpdesk”, “service desk”...). Ce service tient une liste des équipements et de leurs détenteurs, il note et conserve les dates d’attribution et de retrait, les droits d’accès, les modifications et les mises à jour.

Diffamation

- La diffamation est une allégation en relation avec un fait susceptible de porter préjudice à la personne à qui le fait est imputé. La diffamation est parfois distinguée de l’injure (insulte ou outrage) laquelle n’est pas en relation avec un fait présumé. Dans de nombreux pays, la diffamation et l’injure sont des infractions pénales.

- **Risques** : Risque pénal pour l’auteur de la diffamation ou de l’injure, risque pénal pour l’entreprise (notamment, en cas d’utilisation de ses systèmes d’information). Risque réputationnel pour la victime comme pour l’auteur de la diffamation.

• **Protection de l'information** : Les collaborateurs doivent être attentifs à ne pas se rendre coupable de diffamation ou injure. Dans le cas où un collaborateur ou une entité du Groupe est victime d'injures ou de diffamation, le collaborateur qui s'en aperçoit doit contacter son supérieur hiérarchique. Les services juridiques du Groupe sont en charge de gérer ces situations.

• **Protection de l'identité** : Il est interdit de dissimuler son identité dans le but de proférer des injures ou de diffamer.

• **Consigne** : Les collaborateurs doivent être informés sur les risques liés à l'injure et la diffamation. Ces risques concernent à la fois l'auteur et son entreprise.

Donnée

• Une donnée est un élément conventionnel représentant un fait ou une chose. Une ou plusieurs données forment une information. Les données sont enregistrées, c'est-à-dire mises en mémoire, sous diverses formes : papier, image, numérique, analogique...

• **Risques** : Les principaux risques sont la diffusion de données à des personnes qui ne devraient pas les avoir (droits d'accès mal attribués, fuites, vols), la perte de données (bogue, erreur humaine), l'altération de données et leur suppression volontaire (dans le but de nuire ou de faire disparaître des preuves) et le maintien de données inexactes (dans le système d'information) par suite d'une défaillance de leur mise à jour.

• **Consigne** : Les risques doivent être connus des collaborateurs, lorsque ceux-ci constatent un "incident" (voir ce mot), ils doivent le signaler à leur supérieur hiérarchique, ou à la personne responsable de la sécurité informatique.

Droits d'accès

Voir "autorisation d'utilisation".

E-mail

• Un message électronique transféré par Internet ou Intranet (on parle en français de "courriel", de "mél", de "courrier électronique").

• **Risques** : Erreur d'adressage, erreur dans les documents joints, interception du message, perte de confidentialité. Transport de virus et autres logiciels malveillants. Recherche de responsabilité de l'auteur du message et/ou de son entreprise en cas de message inapproprié (diffamation, harcèlement, propos racistes...). Par ailleurs, le système Internet ne garantit pas à 100 % ni les délais, ni la livraison du message à l'adresse indiquée.

• **Protection de l'information** : Un e-mail est très vulnérable. Il ne faut jamais envoyer un message confidentiel par ce moyen (à moins qu'il ne soit encrypté). Ne pas utiliser de renvoi automatique de votre courrier électronique vers un site Internet. Les e-mails de l'entreprise doivent être accompagnés d'un texte rédigé par le service juridique ("disclaimer") pour limiter la responsabilité de l'entreprise en cas de mésusage de l'e-mail.

• **Protection de l'identité** : Il est interdit de cacher votre identité lorsque vous envoyez un e-mail. Ne pas utiliser les adresses e-mail d'un collègue ou d'un tiers, ne jamais autoriser un tiers à utiliser votre propre adresse. Les systèmes d'information et/ou serveurs conservent toujours une trace des e-mails que vous envoyez et que vous recevez, même si vous les faites disparaître de vos listes de messages.

• **Protection du matériel / processus** : éviter d'ouvrir les e-mails provenant de personnes que vous ne connaissez pas (pour limiter le risque de virus). Ne contribuez pas à la réexpédition des lettres-chaîne, des pétitions ni à d'autres actions de "mass mailing" qui encombrant le réseau. Les e-mails trop longs ou avec trop de pièces attachées ralentissent les systèmes de transmission, utilisez la "compression" de fichier (exemple : winzip).

- **Consigne** : Les collaborateurs disposant d'une messagerie électronique doivent connaître les bonnes pratiques et la "Netiquette" (bons usages de l'Internet). Notamment, la longueur autorisée des e-mails et les limites d'utilisation à des fins privées de la messagerie mise à sa disposition par l'entreprise et les risques d'interception par des personnes qui ne sont pas destinataires. Tout message envoyé à partir d'une adresse désignant l'entreprise ne peut contenir que des informations relatives à un usage professionnel. Il est évidemment interdit d'utiliser les systèmes d'information de l'entreprise pour envoyer des messages dont le contenu serait susceptible de porter atteinte à la réputation ou la dignité d'autrui, ayant un caractère raciste, sexiste, révisionniste, discriminatoire, ou dans un but de propagande politique, philosophique ou religieuse, et, d'une manière générale, pour un motif autre que professionnel.

Encryptage (chiffrement)

- L'encryptage (le chiffrement) est une action de masquage des données par utilisation d'une clé de manière à ce que seuls les détenteurs de cette clé puissent décrypter (déchiffrer) les données.
- **Risques** : Connaissance des clés d'encryptage par des personnes non autorisées. Dans certains pays, certains modes d'encryptage sont illégaux.
- **Protection de l'information** : Les e-mails confidentiels échangés à travers internet devraient toujours être chiffrés. Demandez les informations sur l'encryptage au support informatique, ("support utilisateur", "helpdesk", "service desk").
- **Protection de l'identité** : L'encryptage ne doit pas être utilisé pour dissimuler l'identité de l'émetteur au destinataire.
- **Protection du matériel** : Les clés d'encryptage doivent être conservées au coffre ou dans votre tête.
- **Consigne** : Les collaborateurs qui utilisent l'encryptage doivent connaître la réglementation locale le concernant et les modes de protection des clés d'encryptage.

Les fichiers classifiés (voir le mot classification) "Diffusion restreinte" ou "Strictement Confidentiel" doivent être cryptés lors des échanges (exemple : utilisation du ZIP codé, voir ce mot). En pratique, l'encryptage est peu utilisé à cause des difficultés liées au processus. On peut également éviter qu'un document soit altéré en l'envoyant au format pdf.

Espionnage

- Dans le monde des affaires, il est nécessaire d'accumuler des informations sur ses concurrents ou ses fournisseurs. L'obtention de ces informations doit être licite même si elle peut se faire à l'insu de l'entreprise observée. Le terme espionnage est réservé à l'utilisation de moyens non légaux ou non éthiques. Le Groupe n'autorise pas l'utilisation de moyens contestables, tels que : dissimulation/usurpation d'identité, intrusion, vol de document, subordination d'un salarié de l'entreprise, logiciels espions, mouchards de clavier ("keyloggers").
- **Risques** : Pour la victime : vol d'informations confidentielles, perte d'avantages compétitifs, impossibilité de mener une stratégie, chantage. De leur côté, l'espion et/ou son commanditaire courent des risques réputationnels, civils et pénaux.
- **Protection de l'information** : La première règle à respecter est celle de la discrétion, surtout dans les lieux publics. Il faut aussi s'assurer en permanence de la protection physique des documents sensibles. Utiliser des logiciels de protection (exemple : encryption). Méfiez-vous des inconnus qui vous abordent pour vous demander des renseignements sur votre entreprise ou votre métier.
- **Protection de l'identité** : Soyez discret sur votre appartenance à l'entreprise dans les lieux publics ; évitez d'aborder des sujets ou conversations professionnels dans ces lieux.

• **Protection du matériel** : En évitant de donner accès à vos équipements à des tiers, vous limitez les occasions d'y installer des "mouchards", tels que systèmes d'écoute ou de lecture à distance, où qu'ils soient utilisés à d'autres fins illicites.

• **Consigne** : Les collaborateurs du Groupe doivent savoir qu'une grande entreprise est toujours la cible d'espions (agents de certains pays ou d'autres organisations, entreprises et institutions). Des actions de sensibilisation doivent être menées périodiquement. Le Groupe n'utilise que des moyens licites et éthiques pour obtenir des renseignements sur des individus ou des organisations (entreprises, associations, institutions...). Le Groupe réprovoque toute forme d'espionnage industriel.

Fax

• Appareil permettant l'envoi de la copie ("fac-simile") d'un document à distance. Le terme désigne aussi la copie ainsi obtenue. Ces appareils ont souvent une fonction "photocopieuse" (voir ce mot). Les fonctions scanner et messagerie des systèmes d'information remplissent les mêmes fonctions.

• **Risques** : Consultation des documents par des personnes qui ne sont pas les destinataires (mauvaise adresse du destinataire, abandon momentané des documents sur ou à proximité de l'appareil). Vol des documents quand l'appareil ne fait pas l'objet d'une surveillance permanente. Installation de dispositif d'écoute téléphonique, "piratage" (voir ce mot) de l'appareil.

• **Protection de l'information** : Retirer les documents dès réception afin de limiter indiscretions et vols.

• **Protection de l'identité** : S'assurer des coordonnées téléphoniques ou adresses e-mail des destinataires. Prévoir une confirmation téléphonique des adresses avant l'envoi de documents confidentiels (dans ce cas, le courrier est un moyen plus sûr).

• **Protection du matériel** : Il est préférable d'éviter d'installer les fax en "libre-service", sans surveillance. (Faire vérifier par des experts, périodiquement, si les appareils ne sont pas sur écoute.)

• **Consigne** : Les collaborateurs doivent connaître les risques liés aux fax.

Forum de discussion ou de sondage (newsgroup)

• Site Web où il est possible de laisser un commentaire et de lire tous les commentaires des autres personnes qui se sont connectées à ce site et/ou d'avoir des renseignements statistiques sur les réponses.

• **Risques** : Virus, mais surtout risque d'indiscrétion, de diffamation, de harcèlement, de propos/messages inappropriés, rumeur, perte de confidentialité, non-respect de la vie privée, dissimulation, voire usurpation d'identité. Irresponsabilité liée à l'anonymat, le cas échéant.

• **Protection de l'information** : Il faut être vigilant sur les informations échangées sur un forum. Comme ce type de discussion est public, vos commentaires peuvent être exploités à votre rencontre ou à l'encontre de votre entreprise par des personnes mal intentionnées.

• **Protection de l'identité** : L'usage de pseudonyme (ou alias) est fréquent sur les forums. Les collaborateurs du Groupe n'utilisent pas de pseudonyme pour cacher leur identité dans un cadre professionnel.

• **Protection du matériel / processus** : Afin d'éviter tout détournement du processus, le Groupe déconseille de se connecter à des forums à partir de ses systèmes d'information. Ceci peut être interdit dans certaines entités du Groupe : consulter les règles locales.

- **Consigne** : Les collaborateurs doivent savoir que la connexion à un forum est déconseillée à partir des systèmes d'information du Groupe. La connexion à des forums abordant des sujets professionnels peut faire l'objet de dérogation, avec l'autorisation du supérieur hiérarchique assorties des conditions de connexion. Ces conditions ne peuvent pas autoriser la dissimulation d'identité.

Fraude

- Une fraude est commise quand un collaborateur du Groupe agit ou s'abstient d'agir en contradiction avec les réglementations (externes et/ou internes) le concernant. Une fraude est une forme de "non-compliance".
- **Risques** : Disciplinaires, civils et pénaux. Risque réputationnel.
- **Protection de l'information** : Les fraudes les plus fréquentes sont les consultations de sites interdits, les malversations et autres cybercrimes (voir ce mot), les divulgations d'informations confidentielles ou de fausses informations.
- **Protection de l'identité** : L'interdiction de dissimulation d'identité est un principe de responsabilité et de traçabilité. Accéder à un matériel ou un processus sans autorisation d'accès est une fraude.
- **Protection du matériel / processus** : Un collaborateur qui utilise un matériel ou processus sans y être autorisé commet une fraude.
- **Consigne** : Le Groupe effectue des audits périodiques pour évaluer les fraudes et/ou vérifier l'absence de fraude. Ces audits portent, notamment, sur les conditions d'usage des systèmes d'information du Groupe.

Identifiant ("login", code, mot de passe)

- Un identifiant est constitué des informations permettant à une personne d'être reconnue par un système. Le processus d'authentification permet de s'assurer que la personne qui s'identifie est bien celle qu'elle prétend être (exemples : un identifiant tel que nom d'utilisateur et son mot de passe associé ou encore des données biométriques telles que empreintes digitales ou rétinienne, voix...)
- **Risques** : Perte de la confidentialité des données d'authentification (exemple : identifiant et mot de passe associé) par suite d'une protection insuffisante, usurpation d'identité, perte de contrôle des autorisations d'accès. "Les mêmes risques que la perte ou le vol de votre portefeuille et/ou de la clé de votre maison !"
- **Protection de l'information** : Ne jamais communiquer mot de passe à un tiers. "Le seul endroit où il devrait être archivé, c'est dans votre tête", quand cette recommandation n'est pas applicable, voyez avec le support informatique ("support utilisateur", "helpdesk", "service desk"...) la solution la plus acceptable pour gérer vos mots de passe.
- **Protection de l'identité** : Changer périodiquement tous vos mots de passe, ne les inscrivez pas sur un support papier (à moins qu'il ne soit sous clé) ou dans un fichier (à moins qu'il ne soit crypté). En cas d'absence, ne les transmettez à personne ; "c'est comme lui donner votre portefeuille et les clés de votre maison !". Si, exceptionnellement, vous devez un mot de passe à quelqu'un pendant votre absence, changez-le dès votre retour. Faites de même dès que vous soupçonnez quelqu'un de connaître l'un de vos mots de passe.
- **Protection du matériel / processus** : Ne jamais laisser vos mots de passe accessibles à proximité des matériels, les mémoriser ou les mettre sous clé.
- **Consigne** : Les collaborateurs doivent connaître les règles de protection des mots de passe (les meilleures règles de protection varient en fonction des matériels et des logiciels), interroger le support informatique ("support utilisateur", "helpdesk", "service desk"...).

Identité

- Caractère de ce qui est propre à une personne ou à une entité et qui permet de la distinguer des autres.
- **Risques** : Usurpation et dissimulation d'identité, escroquerie, chantage.
- **Protection de l'information** : Chacun doit assumer ses dires et ses actes, il ne peut donc pas dissimuler son identité soit en usurpant celle de quelqu'un d'autre, soit en utilisant un pseudonyme dans le but d'écarter sa responsabilité. Il faut être prudent et discret lorsqu'on échange des informations avec une personne que l'on ne connaît pas. Attention aux erreurs d'adresse (surtout avec les envois d'e-mails) et aux personnes qui camouflent leur identité afin d'obtenir des informations (par exemple : un de vos mots de passe, votre numéro de carte de crédit et son code secret, voir "phishing").
- **Protection de l'identité** : Le Groupe reconnaît à toute personne physique le droit de protéger les données à caractère personnel concernant son identité.
- **Consigne** : Les collaborateurs doivent savoir protéger leurs identifiants et appliquer des règles de vigilance, de prudence et de discrétion dans leurs relations avec des interlocuteurs peu ou mal identifiés.

Imprimante

- L'imprimante est un équipement périphérique commandé à partir de l'ordinateur qui permet de reproduire des textes et des images sur support papier ou autre. De nombreuses imprimantes comportent des fonctions "fax" (voir ce mot) et/ou "photocopieuse" (voir ce mot).
- **Risques** : Consultation des documents imprimés par des personnes non autorisées, perte de confidentialité. Vol du matériel et des ramettes de papier.
- **Protection de l'information** : Une imprimante peut être partagée par plusieurs postes de travail (ordinateurs). Dans ce cas, les utilisateurs doivent rapidement aller chercher les documents imprimés afin de limiter le risque d'indiscrétion. Lorsque vous avez la possibilité d'utiliser plusieurs imprimantes, demandez au Support informatique ("support utilisateur", "helpdesk", "service desk"...) de n'avoir accès qu'à celle qui est la plus proche de votre bureau.
- **Protection du matériel** : Protéger du vol. Utiliser des rames de 500 feuilles minimum pour dissuader les voleurs de papier.
- **Consigne** : L'utilisation des imprimantes partagées doit faire l'objet d'une grande discipline : les documents imprimés doivent être retirés le plus vite possible du bac de l'imprimante. Le collaborateur qui aperçoit un document oublié doit, soit le détruire, soit en avvertir son propriétaire si celui-ci est identifiable.

Incident

- Un incident technique ou comportemental. L'origine d'un dysfonctionnement peut être dû à une défaillance du matériel ou à une défaillance humaine, dans les deux cas celui qui constate le dysfonctionnement doit prendre des mesures de sauvegarde et/ou de correction. Lorsqu'il n'est pas en mesure d'agir, il doit alors avvertir soit son supérieur hiérarchique, soit le service de la maintenance informatique ("support utilisateur", "helpdesk", "service desk"...).
- **Signalement / reporting des incidents** : Si vous n'êtes pas en mesure de traiter un incident, vous devez alors la signaler soit à votre supérieur hiérarchique, soit au service compétent. Si ces derniers ne traitent pas l'incident, vous devez recourir ("rapporter" ou "signaler" le dysfonctionnement) aux instances prévues pour cela comme le service juridique, le compliance officer ou le déontologue. Les personnes à qui on reporte les dysfonctionnements ne sont pas forcément les personnes qui les traitent.

- **Traitement d'une anomalie** : Les personnes en charge d'un matériel ou d'un processus sont les personnes chargées de traiter ces incidents. Quand un incident n'est pas traité ou pas traité convenablement, les personnes qui s'en aperçoivent peuvent recourir au "signalement" (voir ce mot).
- **Consigne** : Les utilisateurs doivent pouvoir traiter par eux-mêmes les incidents les plus fréquents et connaître les procédures de signalement.

Information

- Une information est constituée d'une ou de plusieurs données susceptibles d'être traitées, archivées, transmises. L'ensemble des informations possédées par une entreprise et ses collaborateurs forme un patrimoine dont la valeur contribue au développement économique et social de l'une et des autres. La protection de ce patrimoine est assurée par un "dispositif de sécurité de l'information" dans lequel chaque collaborateur a un rôle à jouer.
- **Risques** : Conséquences d'une modification ou divulgation inappropriée de l'information (exemple : suite à un vol), ou encore d'une cause d'indisponibilité de l'information.
- **Protection de l'information** : Les règles de protection varient en fonction des matériels et processus utilisés pour créer, transmettre ou stocker cette information, ainsi qu'en fonction de leur niveau de "confidentialité" (voir le mot classification).
- **Protection de l'identité** : L'authentification (voir le mot "identifiant") des personnes accédant à une information est un point capital pour assurer la sécurité de l'information (exemple : pensez à vérifier périodiquement la protection des mots de passe).
- **Protection du matériel** : Les équipements où les informations sont stockées doivent faire l'objet de mesures de sécurités appropriées à la nature des équipements et proportionnées au niveau de confidentialité recherché pour les informations. Par exemple : ne jamais laisser sans surveillance un porte-documents ou un ordinateur portable sur un siège (train, voiture, salle de réunion), ne jamais laisser son ordinateur allumé sans surveillance.
- **Consigne** : Les collaborateurs doivent être capables d'identifier les domaines où ils sont concernés par le dispositif de sécurité de l'information du Groupe. Chaque collaborateur doit participer aux actions de formation sur la sécurité de l'information sous la responsabilité de son supérieur hiérarchique.

Intégrité

- Dans le domaine des systèmes d'information, l'intégrité est le caractère d'une information qui n'est pas altérée par un défaut de fonctionnement du système ou par un utilisateur (volontairement ou involontairement).
- **Risques** : Déformation de l'information, escroquerie, faux en écriture, usage de faux, plagiat.
- **Protection de l'information** : Être attentif à ne pas modifier volontairement ou non des informations, notamment lorsque vous transférez un e-mail. Si vous êtes l'auteur d'une modification, indiquez-le.
- **Protection de l'identité** : Pour éviter le plagiat, il est recommandé de citer vos sources et de retranscrire fidèlement les informations.
- **Protection du matériel** : L'adjonction d'équipements ou de logiciel sans l'accord du service de support informatique ("support utilisateur", "helpdesk", "service desk"...) peut provoquer des défauts d'intégrité et entraver le bon fonctionnement des systèmes d'information.
- **Consigne** : Les collaborateurs doivent savoir qu'ils sont responsables de l'intégrité des informations qu'ils transmettent.

Internet

• Ensemble de matériels et de logiciels publics ou privés utilisant un référentiel d'échange commun (protocole TCP/IP) qui permet à tout ordinateur utilisant ce protocole de communiquer avec un autre ordinateur partout dans le monde en vue d'échanger de l'information (exemple : fichiers, images, sons). Le "Web" (voir ce mot), la messagerie (voir "e-mail"), le partage de fichiers à distance sont des applications d'Internet (abréviation d'Interconnected Networks).

• **Risques** : Non-respect des droits d'auteurs, connexion à des sites illégaux, erreurs d'adressage, perte de confidentialité... L'interconnexion facile et générale entraîne de nombreux risques (messages non sollicités, usurpation d'identité, escroquerie, vols, intrusion, espionnage, chantage, phishing...).

• **Protection de l'information** : Seul l'encryptage peut procurer un niveau acceptable de confidentialité. Respectez les règles liées au niveau de confidentialité de l'information (voir "classification de l'information"). N'échangez que des informations professionnelles à partir d'une adresse professionnelle. Comprimez les gros fichiers et lancez leur transfert en dehors des périodes de forte activité (contactez votre support informatique "support utilisateur", "helpdesk", "service desk"...)

• **Protection de l'identité** : Ne donnez votre adresse e-mail qu'aux personnes en qui vous avez confiance. Ne donnez jamais les coordonnées, ni les mots de passe d'un intranet ou Extranet d'une entreprise du Groupe. Ne divulguiez jamais vos mots de passe sur Internet.

• **Protection du matériel / processus** : Les réseaux sont le véhicule habituel de virus, chevaux de Troie, spams, etc. Les réseaux des entreprises sont bien protégés contre ces risques, évitez de connecter votre équipement sur un réseau non sécurisé (exemple : réseaux Wi-Fi publics). Ne connectez jamais votre équipement sur deux réseaux simultanément (exemple : le réseau de l'entreprise et un réseau Wi-Fi).

• **Consigne** : Les collaborateurs doivent connaître la manière la plus sûre d'utiliser les applications de l'Internet (Web, messagerie...). Ils doivent aussi savoir que l'entreprise a mis en place des outils pour surveiller l'usage des services Internet. Ces outils permettent notamment le contrôle des pratiques (adresses des messages, sites visités, date et heure, durée d'utilisation).

Malware (logiciel malveillant)

• Ensemble de programmes conçus pour s'installer insidieusement dans un système afin d'y déclencher une opération non autorisée, de l'endommager ou d'en perturber le fonctionnement. Par exemple : collecte frauduleuse d'informations, modification ou destruction de données. Exemples de malware : bombe programmée, virus, vers, cheval de Troie, "key logger", "rootkit", "spyware"...

• **Risques** : Panne de l'ordinateur "contaminé", voire panne de l'ensemble du réseau. Perte de la confidentialité. Perte d'informations. Chantage.

• **Protection de l'information** : Les logiciels malveillants peuvent être transmis via Internet ou un réseau local, voire par des supports tels que les disquettes, les clés USB ou les Cd-roms,

• **Protection de l'identité** : Le vol des identifiants et des mots de passe sont un des principaux objectifs des malware, cette activité de piratage est très fréquente.

• **Protection du matériel / processus** : Les équipements informatiques doivent être équipés de logiciels spécialisés anti-malware.

• **Consigne** : Tout collaborateur qui soupçonne la contamination de son ordinateur doit avertir le support informatique ("support utilisateur", "helpdesk", "service desk"...), déconnecter son équipement du réseau pour éviter la diffusion d'un virus mais éviter d'arrêter l'ordinateur afin de faciliter les investigations ultérieures.

Messagerie électronique

Voir e-mail.

Metadonnées

- Aussi appelées “métadatas”, il s’agit, entre autre, des informations contenues dans un fichier (modifications du document, suppressions d’éléments, ajout de contenus...) qui constituent l’historique du document et qui peuvent être accessibles alors même que l’auteur les pense invisibles. Les métadonnées sont utilisées pour faciliter la compréhension, les caractéristiques, l’utilisation et la gestion de données sur tout type de support. Elles varient selon le type d’information et le contexte de leur utilisation. Dans le cadre des systèmes d’information les métadonnées sont constituées par le contenu des fichiers informatiques, elles comprennent aussi généralement le nom du fichier, le type de fichier, le nom de l’auteur et la classification des données.

- **Risques** : Si vous envoyez un document non protégé (word, excel, PPT...), le destinataire peut être en mesure de retrouver des informations qui ont été révisées ou supprimées (ex. : modification d’un prix de soumission d’une indemnité spéciale ou d’autres clauses, modifications dans le cadre de négociations et de litiges sensibles...). Dans des documents réalisés avec Sharepoint ou Office de Microsoft, les métadonnées peuvent contenir le nom de l’auteur, le nom de la dernière personne à avoir modifié le fichier, le nombre d’impressions du document, le nombre de révisions apportées au document, les parties supprimées... Certaines métadonnées sont invisibles pour un utilisateur normal, mais peuvent être récupérées à l’aide de logiciels d’analyse spécialisés. L’inclusion par inadvertance de ces informations dans des fichiers diffusés provoque parfois des complications juridiques pour les entreprises lorsque ces informations sont utilisées dans le cadre de poursuites judiciaires.

- **Consigne** : Les utilisateurs doivent être conscients que, dans la mesure du possible sur le plan technique, les métadonnées doivent être supprimées des documents par l’auteur avant que ces derniers ne soient communiqués (par ex. : création d’un fichier .pdf à partir d’un document typique réalisé dans Microsoft Office). Dans des cas extrêmes, certains logiciels spécialisés permettent de nettoyer les métadonnées des documents avant que ces derniers ne soient envoyés en dehors de l’entreprise. Les utilisateurs doivent contacter leur support informatique (“support utilisateur”, “help desk”, “service desk”) s’ils ont besoin d’aide.

Modification des informations

- Des informations peuvent être mises à jour, soit parce que les faits s’y rattachant ont changé, soit parce que l’interprétation de ces faits a évolué.

- **Risques** : Faux en écriture, plagiat, perte de confidentialité, infraction à la protection des droits de propriété intellectuelle (copyright, marques déposées...).

- **Protection de l’information** : Pour qu’une information soit modifiée par un collaborateur il faut (1) que ce dernier soit habilité à le faire et (2) que la modification ne constitue pas une erreur ni ne transgresse les droits de propriété intellectuelle.

- **Protection de l’identité** : Lorsque l’on emprunte une information à quelqu’un, il faut en faire état. Lors d’une modification de texte, on ne peut s’attribuer un texte écrit par quelqu’un d’autre ni même omettre de citer l’auteur. On ne peut non plus modifier un document appartenant à quelqu’un sans sa permission.

- **Protection du matériel / processus** : L’encryptage de l’information peut se révéler nécessaire pour protéger son intégrité. Veillez à respecter les règles de la politique de classification (voir “classification de l’information”).

- **Consigne** : Les collaborateurs doivent connaître les règles de respect de l’intégrité des informations.

Modification des matériels

- Les matériels mis à la disposition des collaborateurs sont définis par la DSI de l'entreprise de manière à assurer la compatibilité de tous les éléments du système d'information. La forte imbrication de toutes les composantes fait qu'un défaut de l'une d'elle peut avoir des répercussions sur la sécurité de nombreux autres éléments du système. Pour cette raison, il est interdit à un collaborateur de connecter un matériel ou d'importer un logiciel sur les équipements mis à sa disposition sans l'accord du support informatique ("support utilisateur", "helpdesk", "service desk"...).

- **Risques** : Panne des équipements, détérioration, blocage des échanges d'information, perte de confidentialité, perte d'information.

- **Protection de l'information** : Ne jamais modifier le matériel mis à votre disposition par l'entreprise. Ne pas ajouter des équipements ou des logiciels (même gratuits) de votre propre initiative.

- **Protection de l'identité** : Les modifications de matériels comme celles des logiciels peuvent invalider les protections d'identité (par contournement des processus d'authentification).

- **Protection du matériel** : L'ajout d'équipements peut détériorer les matériels.

- **Consigne** : Les collaborateurs doivent connaître le danger d'une modification de matériel ou des logiciels mis à leur disposition.

Mot de passe

- Un mot de passe est un élément permettant l'authentification d'un utilisateur (voir "identifiant").

- **Risques** : Perte de la confidentialité d'un mot de passe par suite d'une protection insuffisante, usurpation d'identité, perte de contrôle des autorisations d'accès. "Les mêmes risques que la perte ou le vol de votre portefeuille et/ou de la clé de votre maison !".

- **Protection de l'information** : Ne jamais communiquer un mot de passe à un tiers. "Le seul endroit où il devrait être archivé, c'est dans votre tête", quand cette recommandation n'est pas applicable, voyez avec le support informatique ("support utilisateur", "helpdesk", "service desk"...) la solution la plus acceptable pour gérer vos mots de passe.

- **Protection de l'identité** : Changer périodiquement vos mots de passe, ne les écrivez pas sur un support papier (à moins qu'il ne soit sous clé) ou dans un fichier (à moins qu'il ne soit crypté). En cas d'absence, éviter de les transmettre à un tiers : "c'est comme lui donner votre portefeuille et les clés de votre maison !". Si, exceptionnellement, vous devez laisser votre mot de passe à quelqu'un pendant votre absence, changez-le dès votre retour. Faites de même dès que vous soupçonnez quelqu'un de connaître l'un de vos mots de passe.

- **Protection du matériel / processus** : Ne jamais laisser les mots de passe accessibles à proximité des matériels, les mettre sous clé, ou mieux les mémoriser.

- **Consigne** : Les collaborateurs doivent connaître les règles de sécurisation des mots de passe et protéger leurs identifiants (les meilleures règles de protection varient en fonction des matériels et des logiciels), interrogez votre support informatique ("support utilisateur", "helpdesk", "service desk"...). Les mots de passe sécurisés sont composés au minimum de huit caractères et d'un mélange de majuscules, de minuscules, de chiffres et surtout de signes tels que : " ! & @ # \$ % ^ ? ...

Mutation (de personnel)

- Les collaborateurs peuvent recevoir de nouvelles missions, être déplacés ou quitter l'entreprise. Tout ceci doit entraîner une nouvelle définition des informations à mettre à leur disposition (droits d'accès).
- **Risques** : Perte et vol de données. Perte de confidentialité. Divulgence d'informations personnelles. Droits d'accès non pertinents.
- **Protection de l'information** : En cas de mutation, les données mises à la disposition du collaborateur doivent être analysées, et l'accès à des données non pertinentes (en fonction de la nouvelle affectation) doit être rendu impossible.
- **Protection de l'identité** : Les droits d'accès doivent être redéfinis à chaque mutation.
- **Protection du matériel** : Les matériels et leurs détenteurs doivent être identifiables, car les détenteurs sont responsables de leur matériel. Des mises à jour s'imposent à chaque mutation.
- **Consigne** : Le service capable de vérifier les droits d'accès est le support informatique ("support utilisateur", "helpdesk", "service desk"...). Ce service possède une liste des équipements et de leurs détenteurs.

Ordinateur

- Matériel informatique capable de traiter des données, son utilisation nécessite habituellement des outils "périphériques" : clavier, écran, imprimante... Cet ensemble forme alors un "poste de travail informatique".
- **Risques** : Détérioration, panne, vol, perte.
- **Protection de l'information** : L'accès aux informations contenues sur un ordinateur doit être protégé afin que celles-ci soient disponibles aux seuls utilisateurs autorisés, dans leur intégralité et en permanence.
- **Protection de l'identité** : L'accès aux informations d'un ordinateur doit être protégé par un mot de passe (ou un dispositif équivalent) permettant l'authentification de l'utilisateur. Un ordinateur ne doit pas rester en service hors de la présence de son (ou ses) utilisateurs autorisés (voir verrouillage écran).
- **Protection du matériel** : Le vol d'ordinateur est motivé par son contenu autant que par la valeur de l'objet proprement dit.
- **Consigne** : Tout collaborateur ayant accès à un ordinateur doit être sensibilisé au dispositif de sécurité de l'information du Groupe. Informez-vous auprès du support informatique ("support utilisateur", "helpdesk", "service desk"...)

PDA

Voir "agenda électronique".

Pédophilie

- Le fait de fabriquer, détenir, transmettre, diffuser des images de pornographie représentant des enfants (ou des personnes en ayant l'aspect physique) est une activité criminelle dans la plupart des pays.
- **Risques** : Condamnation pénale (prison, amende) des personnes s'adonnant aux activités définies ci-avant, dans les pays où la loi le prévoit (notamment dans l'Union Européenne et aux États-Unis). Risque réputationnel dans tout pays.
- **Protection de l'information** : Il est interdit d'utiliser les systèmes d'information de l'entreprise dans le cadre des activités définies ci-avant, que ces systèmes soient situés ou non dans des pays qui incriminent la pédophilie.

- **Protection de l'identité** : Des services de police traquent les utilisateurs de sites pédophiles. Ces services réussissent à repérer des pédophiles, même lorsque ceux-ci utilisent des procédés de cryptage pour dissimuler leurs messages et leur identité.

- **Consigne** : Les collaborateurs doivent savoir qu'il est interdit d'utiliser les systèmes d'information du Groupe pour effectuer des activités illégales. Par ailleurs, et par mesure de précaution, les collaborateurs doivent également savoir qu'ils ne sont pas autorisés à utiliser les équipements des systèmes d'information de l'entreprise (pendant ou en dehors des heures de travail) pour consulter des sites à caractère pornographique ou érotique, même tolérés par la réglementation.

Piratage

- Le piratage est une intrusion dans un système informatique afin d'y dérober ou de modifier des informations, voire de le rendre indisponible.

- **Risques** : Vol, escroquerie, falsification et destruction de données, perte de confidentialité...

- **Protection de l'information** : Penser à faire des sauvegardes (voir ce mot) pour ne pas perdre des informations. Quand vous êtes sur le réseau de l'entreprise, votre ordinateur est protégé du risque d'intrusion ; mais cela n'est plus le cas si vous vous connectez sur un réseau non sécurisé (par exemple, un réseau Wi-Fi public).

- **Protection de l'identité** : Le vol des identifiants et des mots de passe est une activité de piratage très fréquente.

- **Protection du matériel / processus** : Le piratage n'a pas d'influence sur le matériel proprement dit.

- **Consigne** : Les utilisateurs d'équipements portables (PC, smartphone) doivent être sensibilisés aux risques de piratage lorsqu'ils s'en servent en dehors du bureau.

Phishing

- Envoi d'e-mails proposant aux destinataires de fournir des données personnelles (N° carte bancaire, code secret, mot de passe, date de naissance...) sur un faux site Web contrefaisant un site officiel (par exemple celui de la banque du destinataire ou d'une autre institution).

- **Risques** : Escroquerie.

- **Protection de l'information** : Seule compte la vigilance de l'internaute, une entreprise ou une institution ne demanderont par exemple jamais l'envoi de données confidentielles ou la modification d'un mot de passe par l'intermédiaire d'un e-mail.

- **Protection de l'identité** : Seule compte la vigilance de l'internaute.

- **Consigne** : Les collaborateurs doivent être périodiquement sensibilisés aux risques de phishing et à l'interdiction de répondre aux "spams" (voir ce mot).

Photocopieuse / photocopies

- Machine servant à dupliquer des documents papier. Souvent combiné avec une fonction "imprimante" (voir ce mot) ou "fax" (voir ce mot).

- **Risques** : Consultation des documents imprimés par des personnes non autorisées. Perte de confidentialité. Autres risques : vol du matériel et/ou des ramettes de papier.

- **Protection de l'information** : Les utilisateurs doivent veiller à ne pas laisser de documents dans, ou à côté de la machine afin de limiter le risque d'indiscrétion.

- **Protection de l'identité** : Certaines machines exigent d'entrer un code pour fonctionner.

- **Protection du matériel / processus** : Utiliser des ramettes de 500 feuilles minimum pour dissuader les voleurs de papier.
- **Consigne** : Les documents imprimés doivent être retirés le plus vite possible du bac de l'imprimante. Le collaborateur qui aperçoit un document oublié doit soit le détruire, soit en avvertir son propriétaire si celui-ci est identifiable.

Pornographie

- La pornographie englobe toutes les formes de représentation érotique qui peuvent être considérées comme dégradantes pour la dignité humaine ou blessante pour certaines catégories de personnes.
- **Risques** : Risque réputationnel, voire risque pénal liés à certains sites et selon les lois locales (notamment dans l'Union Européenne et aux États-Unis).
- **Protection de l'information** : Les collaborateurs ne sont pas autorisés à utiliser les équipements des systèmes d'information de l'entreprise pour envoyer des messages ou pour consulter des sites à caractère pornographique ou érotique, même tolérés par la réglementation.
- **Protection de l'identité** : Le système d'information de l'entreprise conserve une trace des sites Web visités.
- **Protection du matériel / processus** : Les sites pornographiques et érotiques sont souvent vecteurs de virus.
- **Consigne** : Les collaborateurs doivent savoir qu'ils ne sont pas autorisés à utiliser les systèmes d'information de l'entreprise pour consulter des sites à caractère pornographique ou érotique, même tolérés par la réglementation. Ils doivent également savoir que le système d'information de l'entreprise conserve une trace de toutes les adresses des sites Web qu'ils visitent et que les entités collaborent aux enquêtes diligentées par les autorités administratives ou judiciaires.

Portable (ordinateur, téléphone)

- Par opposition à un équipement fixe, un équipement portable est conçu pour pouvoir accompagner son utilisateur lors de ses déplacements.
- **Risques** : Vol, perte, écoute clandestine, utilisation à l'insu de son détenteur, piratage, chantage.
- **Protection de l'information** : Les informations contenues dans les portables sont moins bien protégées que dans les appareils fixes. Dans les lieux publics, l'utilisation de ces appareils doit se faire avec discrétion.
- **Protection de l'identité** : Toujours utiliser des procédures d'authentification (codes PIN, mots de passe...) pour la mise en marche des appareils portables (téléphone, ordinateur, PDA...). Le vol des appareils non protégés permet la lecture des données personnelles qu'ils contiennent, notamment les carnets d'adresses et les agendas.
- **Protection du matériel** : Surveillez vos équipements portables, mettez-les sous clé lorsque c'est possible (exemple : câble de sécurité pour les ordinateurs portables).
- **Consigne** : Chaque utilisateur d'un appareil portable doit savoir comment protéger les informations qu'ils contiennent ainsi que celles qu'il transmet.

Plainte

- Tout collaborateur qui subit un préjudice (voir ce mot) doit pouvoir s'exprimer à ce sujet. Il en est de même quand un collaborateur est informé, par quelque moyen que ce soit, d'un préjudice subit par une entité du Groupe. Normalement, la personne à contacter est le supérieur hiérarchique du collaborateur, ou une autre personne qualifiée pour cela (Directeur juridique, DRH, Déontologue), ou encore une personne désignée par la réglementation.

- **Risques** : Ne pas réagir face à un préjudice donné entraîne le risque de son renouvellement.
- **Protection de l'information** : La plainte, comme le préjudice dont elle fait l'objet, sont des informations "diffusion restreinte".
- **Protection de l'identité** : A priori, le nom de l'auteur d'une plainte, comme ceux des personnes éventuellement mises en cause sont "diffusion restreinte", dans certains pays (notamment en Europe) ces données ne peuvent figurer dans des fichiers qu'à certaines conditions.
- **Protection du matériel / processus** : Les vols ou détériorations de matériel doivent être portés à la connaissance du support informatique ("support utilisateur", "helpdesk", "service desk"...) et dans certains cas faire l'objet d'une plainte officielle auprès des services de police. Les plaintes doivent être faites de bonne foi.
- **Consigne** : Tous les collaborateurs doivent connaître les règles concernant le dépôt d'une plainte relative à un préjudice subi à leur rencontre, à celle d'une entité du Groupe, voire à celle d'un tiers.

Préjudice encouru par le mésusage

- Un mauvais usage ou une protection inappropriée de l'information peut entraîner un préjudice pour l'entreprise, un collaborateur et/ou un tiers.
- **Risques** : Perte de confidentialité et/ou de compétitivité, risque réputationnel, coût de la réparation, sanction disciplinaire ou administrative, condamnation civile ou pénale.
- **Protection de l'information** : Une règle de base est le "verrouillage" (voir ce mot) des écrans quand on s'absente de son poste de travail ; une autre est de laisser un bureau net de tout document en dehors des heures de travail.
- **Protection de l'identité** : Chaque collaborateur doit veiller à bien gérer ses "identifiant"s (voir ce mot) et mots de passe.
- **Protection du matériel** : Chaque collaborateur est directement responsable du matériel qui lui est confié par l'entreprise, mais il doit aussi se sentir responsable des autres biens appartenants à l'entreprise, car il peut subir un préjudice indirect du fait de leur vol ou de leur détérioration.
- **Consigne** : Les responsables hiérarchiques veillent à l'information et la formation de leurs collaborateurs afin de minimiser les préjudices consécutifs à une mauvaise gestion de l'information et/ou un mésusage des moyens d'information.

Privé (usage du matériel à des fins privées)

- Pour des questions de sécurité et de responsabilité, les collaborateurs ne peuvent utiliser qu'exceptionnellement à des fins privées les systèmes d'information mis à leur disposition par l'entreprise. De la même manière, ils n'utiliseront qu'avec beaucoup de prudence à des fins professionnelles des systèmes d'information qui n'appartiennent pas à l'entreprise.
- **Risques** : Mise en cause de la responsabilité civile et/ou pénale de l'entreprise, perte de confidentialité, piratage, virus.
- **Protection de l'information** : La sécurité des moyens d'information de l'entreprise peut être compromise par l'utilisation de matériels non compatibles.
- **Protection de l'identité** : L'utilisation du matériel par son propriétaire évite toute ambiguïté sur la détermination des responsabilités.
- **Protection du matériel** : L'utilisateur d'un matériel mis à sa disposition par l'entreprise doit prendre soin de ce matériel comme il le fait pour le sien.
- **Consigne** : Les collaborateurs doivent être sensibilisés aux risques liés à l'usage de matériels de communication qui ne sont pas fournis par l'entreprise.

Privé (information à caractère personnel)

• Chaque individu a le droit de protéger sa vie privée (sa photo, les informations sur son histoire, son mode de vie, sa santé, ses proches, ses revenus, ses goûts...). Les données relatives à la vie privée des individus ne peuvent donc pas être diffusées ou utilisées à son insu. Dans de nombreux pays les “données à caractère personnel” font l’objet d’une réglementation relative à leur traitement. Le Groupe respecte ces réglementations dans les pays n’en ayant pas ou ayant une réglementation moins restrictive que la Directive Européenne 95/46/CE du 14 octobre 1995, le Groupe s’inspire de cette Directive pour sa propre réglementation.

• **Risques** : Indiscrétion, exploitation malveillante des informations collectées. Risques de condamnation civile ou pénale dans de nombreux pays.

• **Protection de l’information** : Toujours s’informer sur les réglementations relatives à la protection de la vie privée avant de traiter une information se rapportant à un individu.

• **Protection de l’identité** : Une information à caractère personnel est une information qui permet d’identifier un individu à partir des données qu’elle contient.

• **Consigne** : Les collaborateurs ayant accès à des informations à caractère personnel (service clients, DRH...) doivent connaître les procédures relatives à leur traitement.

Propriété intellectuelle (licences / copyrights / téléchargement)

• La propriété intellectuelle se rapporte aux droits résultant des activités intellectuelles dans le domaine industriel, scientifique ou artistique, par exemple : brevets, licences, marques, droits d’auteur, copyrights (de logiciels, films, vidéos...).

• **Risques** : Plagiat, contrefaçon, perte d’avantages compétitifs.

• **Protection de l’information** : Les objets et informations protégés par des droits d’auteur doivent être utilisés dans le respect de ces droits. Les collaborateurs doivent posséder les autorisations avant utilisation.

• **Protection de l’identité** : Les images, logos et textes protégés par des copyrights ne peuvent être reproduits sans autorisation de l’auteur ou du propriétaire des droits. Les courtes citations sont tolérées lorsque l’auteur est cité.

• **Protection du matériel / processus** : Les autorités ont la faculté de confisquer les matériels ayant servi à la contrefaçon.

• **Consigne** : Les collaborateurs doivent savoir qu’il est interdit de télécharger des œuvres protégées par des droits d’auteur, il est interdit de les copier (contrefaçon, plagiat). Par sécurité, le Groupe interdit de télécharger, sur ses matériels, les logiciels, jeux, films et vidéos, même libres de droits, sauf autorisation du supérieur hiérarchique et du support informatique (“support utilisateur”, “helpdesk”, “service desk”...).

Protection (des données / des matériels / des documents / des locaux)

• L’information que possède une entreprise fait partie de son patrimoine : la protection de l’information ne se limite pas aux seules questions de sécurité informatique ; elle est la résultante d’actions de protection des données, des logiciels mais aussi des matériels, des documents, des “supports amovibles de stockage de données”, des locaux. Sans cet ensemble de protections, l’information devient vulnérable.

• **Risques** : Vol, perte de confidentialité, perte de compétitivité.

• **Consigne** : Les collaborateurs doivent connaître les règles de protection de l’information, c’est-à-dire de la protection des données, des logiciels, des matériels, des documents, des “supports amovibles de stockage de données” et des locaux.

Protection de la vie privée

Voir “privé (information à caractère personnel)”.

Règles applicables

- La gestion des informations détenues par le Groupe est soumise à des règles issues d'obligations externes (Autorités publiques, Agences régulatrices...) et de décisions propres au Groupe et à ses entités.
- **Risques** : Le non-respect des règles peut entraîner de nombreux préjudices pour le Groupe, ses entités et ses collaborateurs ainsi que pour des tiers (les principaux risques sont précisés dans chaque rubrique du présent glossaire)
- **Protection de l'information** : Le non-respect de ces règles de protection a, avec d'autres préjudices possibles, un effet néfaste sur la compétitivité de l'entreprise.
- **Protection de l'identité** : Les règles de protection de l'identité ont à la fois des conséquences pour l'entreprise et pour le collaborateur dont l'identité est usurpée ou dissimulée. Le collaborateur doit également songer à vérifier l'identité de ses interlocuteurs.
- **Protection du matériel / processus** : L'action d'empêcher le vol ou la détérioration du matériel se justifie par elle-même, mais également par les conséquences que cela peut avoir pour la gestion, la transmission et la protection des informations.
- **Consigne** : Chaque collaborateur doit connaître les règles à appliquer pour l'exercice de sa fonction.

Reporting des incidents

- Celui qui constate un dysfonctionnement doit prendre des mesures de sauvegarde et/ou de correction. Lorsqu'il n'est pas en mesure d'agir, il doit alors avertir soit son supérieur hiérarchique, soit le support informatique (“support utilisateur”, “helpdesk”, “service desk”...) ou un autre service compétent : DRH, Service Juridique, Direction de l'Ethique et de la Compliance.
- **Risques** : Le reporting fait de mauvaise foi est une “fraude” (voir ce mot), il peut être un acte de “diffamation” (voir ce mot) ou de “dénigrement” (voir ce mot).
- **Protection de l'information** : Le reporting permet d'évaluer la nature et l'importance des menaces sur la confidentialité, la disponibilité et l'intégrité de l'information. Le reporting doit être fait de bonne foi.
- **Protection de l'identité** : Le reporting permet d'évaluer la nature et l'importance des menaces liées à l'usurpation ou la dissimulation de l'identité des utilisateurs du système d'information de l'entreprise.
- **Protection du matériel** : Le reporting permet d'évaluer la nature et l'importance des menaces concernant les équipements utilisés pour la gestion de l'information.
- **Consigne** : Les collaborateurs doivent savoir à qui rapporter les incidents. Ils doivent également pouvoir faire la distinction entre les personnes à qui ils reportent les dysfonctionnements et les personnes qui sont en charge de leur traitement, car ce ne sont pas forcément les mêmes.

Réseau social

- Le terme de réseau social désigne un ensemble de personnes ou d'organisations réunies par des liens, notamment par des échanges d'informations. En informatique, des applications Internet permettent de rassembler des individus autour d'un thème commun, par exemple : trouver des partenaires commerciaux, un emploi, des anciens collègues... On parle aussi de "services de réseautage social", de "site communautaire", de "site de rencontres", de "réseautique".

- **Risques** : Dissimulation d'identité, atteinte à la vie privée, recoupement d'informations, perte de confidentialité, "espionnage" (voir ce mot), chantage, harcèlement.

- **Protection de l'information** : Les informations délivrées sur des sites de réseau social peuvent être exploitées par recoupement à des fins d'espionnage industriel. C'est la première raison pour laquelle la connexion à ces sites est interdite à partir des systèmes d'information de l'entreprise. Les collaborateurs doivent également être très prudents lorsqu'ils se connectent à ces sites depuis leur propre matériel, afin de ne pas divulguer d'informations confidentielles relatives à leur entreprise, ne pas dénigrer ni diffamer, ni effectuer une quelconque action illicite, ni surtout faciliter des actes dont ils seraient les premières victimes.

- **Protection de l'identité** : La dissimulation d'identité est fréquente sur les sites de réseau social, les informations délivrées sur ces sites facilitent l'usurpation d'identité par des malfaiteurs, voire des actions de harcèlement ou de chantage. C'est la deuxième raison pour laquelle la connexion à ces sites est interdite à partir des systèmes d'information de l'entreprise. Les collaborateurs doivent également être très prudents lorsqu'ils se connectent à ces sites depuis leur propre matériel, afin de ne pas être victime de l'usurpation de leur identité, ni effectuer une quelconque action illicite en dissimulant leur identité.

- **Consigne** : Les collaborateurs doivent connaître les risques liés à l'utilisation de ces sites, ils doivent savoir pourquoi il est interdit de s'y connecter. La connexion à un site de réseau social peut cependant être autorisée par les supérieurs hiérarchiques dans un but professionnel et limité aux seules informations indispensables.

Responsabilité

(Voir aussi "compliance", "préjudice")

- On entend ici le terme "responsabilité" comme l'ensemble des faits qu'un individu (ou un groupe d'individus) doit assumer, dans le cadre d'une mission qu'il a choisie ou acceptée. Chacun est responsable de ses actes et ne peut atténuer sa responsabilité au prétexte qu'il obéit à un ordre de son supérieur (par exemple, si cet ordre était illégal ou incohérent).

- **Risques** : Au sein d'une organisation, les défaillances de responsabilité de certains collaborateurs et/ou une répartition inadéquate des responsabilités peuvent empêcher un fonctionnement éthique et limiter l'efficacité de l'ensemble de l'organisation.

- **Consigne** : Il appartient aux supérieurs hiérarchiques de s'assurer que leurs collaborateurs assument leurs responsabilités et que celles-ci leur sont attribuées de manière adéquate (en fonction de leurs compétences et de leurs moyens, notamment de leur position dans la hiérarchie, les responsabilités doivent être explicitées par un ordre de mission ou une définition de fonction). Les défaillances doivent entraîner des sanctions (voir ce mot) appropriées à leur fréquence et à leur gravité. Les collaborateurs doivent savoir enfin comment agir lorsque des obstacles les empêchent de remplir leurs missions, notamment comment utiliser les voies de recours qui sont à leur disposition.

Sanction (des personnes physiques et des personnes morales)

- La sanction est une conséquence d'une non-compliance (voir ce mot). L'origine de la sanction peut être interne à l'entreprise (sanction disciplinaire, licenciement) ou externe, par exemple judiciaire. Des défaillances dans l'application des règles de Protection des informations et de leurs échanges, des identités ou du matériel peuvent entraîner des sanctions pour les collaborateurs comme pour une entreprise.

- **Risques** : Les sanctions disciplinaires ou judiciaires sont appliquées en fonction de critères prédéfinis ; mais la "non-compliance" peut également avoir des conséquences difficilement estimables : sanctions médiatiques, économiques et réputationnelles d'un coût élevé, entraînant parfois la disparition de l'entreprise (exemple : la disparition du cabinet conseil Arthur Andersen, en 2002).

- **Consigne** : Les sanctions internes ont avant tout un but pédagogique, tandis que les sanctions externes ont plutôt un rôle punitif. Les sanctions internes prennent en compte le principe du droit à l'erreur.

Sauvegarde

- La sauvegarde (on dit aussi : "back-up", "copie de secours", "copie de sécurité") consiste à copier des logiciels et ou des fichiers d'un support (exemple : le disque dur de votre ordinateur ou un serveur) sur un autre support (exemple : un CD, un serveur) afin qu'ils ne soient pas perdus en cas d'incident sur le support d'origine.

- **Risques** : L'absence de sauvegarde régulière des informations de votre ordinateur vous fait courir le risque de les perdre sans possibilité de les retrouver ou de les reconstituer.

- **Protection de l'information** : S'assurer qu'une sauvegarde journalière des informations contenues dans votre ordinateur est effectuée est la meilleure façon de les protéger (c'est-à-dire d'être certain de les retrouver le lendemain), consultez à ce sujet votre support informatique ("support utilisateur", "helpdesk", "service desk"...).

- **Protection de l'identité** : La meilleure sauvegarde de vos identifiants et mots de passe s'effectue dans votre tête.

- **Protection du matériel / processus** : La sauvegarde est aussi une parade à la détérioration ou au vol de votre ordinateur ou de tout autre élément du système d'information de l'entreprise.

- **Consigne** : Les collaborateurs doivent être informés des sauvegardes systématiques opérées par le Service Informatique. Ils doivent également savoir comment gérer les sauvegardes de leurs équipements nomades (portables, PDA, smartphones...).

Sécurité

- La sécurité de l'information est la résultante de plusieurs éléments de sécurité : sécurité des logiciels, sécurité des télécommunications, sécurité des matériels, sécurité de leur environnement (exemple : les locaux) et sécurité des comportements des utilisateurs.

C'est l'ensemble des moyens techniques, organisationnels, juridiques et humains mis en œuvre pour garantir ou rétablir le respect des trois caractéristiques suivantes de l'information :

- Confidentialité : seules les personnes autorisées ont accès à l'information.

- Intégrité : l'information est conservée de façon exacte et complète.

- Disponibilité : Les utilisateurs autorisés ont accès à l'information lorsqu'ils en ont besoin.

La sécurité de l'information impacte l'utilisation des logiciels, matériels, télécommunications, bâtiments ainsi que le comportement des collaborateurs.

- **Risques** : Un défaut de sécurité de l'information augmente les risques financiers, juridiques, réputationnels et opérationnels pour l'entreprise. Les conséquences peuvent être graves alors même que l'incident initial est jugé anodin.
- **Protection de l'information** : Le traitement et l'échange des informations au sein et hors de l'entreprise sont soumis à des règles explicitées dans la politique de classification de l'information Groupe (voir "classification de l'information").
- **Consigne** : Les collaborateurs doivent être sensibilisés aux risques liés à la sécurité de l'information, aux politiques, standards et procédures mis en œuvre pour diminuer ces risques à l'échelle du Groupe et de ses entités.

Serveur

- Un serveur est un système informatique qui fournit des services à ses utilisateurs : mise à disposition de fichiers et applications, stockage de sauvegarde... et ce à travers un réseau.
- **Risques** : Les serveurs constituent des silos d'information, ce qui fait d'eux une cible privilégiée des malfaiteurs.
- **Protection de l'information** : Les serveurs sont généralement protégés par des dispositifs spécifiques de sécurité.
- **Protection de l'identité** : Chaque serveur a des procédures propres d'authentification. Sur Internet, ceux qui offrent des garanties de sécurité sont signalés par le préfixe https://
- **Protection du matériel** : La détérioration d'un serveur impacte la disponibilité des informations pour l'ensemble des ordinateurs susceptibles de s'y connecter.
- **Consigne** : Les collaborateurs doivent savoir comment sauvegarder (voir le mot "sauvegarde") leur travail quotidien sur les serveurs de l'entreprise. Ils doivent également connaître les serveurs Internet interdits d'utilisation.

Signalement

Voir "reporting des incidents".

Site communautaire

Voir "réseau social".

Site de rencontres

Voir "réseau social".

Site interdit

- D'une manière générale, les sites auxquels se connectent les collaborateurs doivent être en relation directe ou indirecte avec leur activité professionnelle. La connexion aux sites suivants est interdite : site illégal, immoral, diffamatoire, révisionniste, prônant la discrimination, pornographique, pédophile, érotique, violent, portant atteinte à la dignité humaine...
- **Risques** : En dehors des sanctions disciplinaires et judiciaires encourues par les collaborateurs, l'entreprise peut encourir un risque réputationnel, elle peut aussi être accusée de complicité et risquer une condamnation. Du matériel peut être mis sous scellés ou saisi.
- **Protection de l'information** : Les serveurs du Groupe peuvent être équipés de systèmes destinés à interdire l'accès aux sites interdits.

- **Protection de l'identité** : Les serveurs permettent d'identifier les origines des connexions. Ceci donne la possibilité aux entités du Groupe de collaborer aux éventuelles enquêtes diligentées par les autorités, dans le cas de consultation de sites interdits.
- **Protection du matériel / processus** : Les autorités peuvent saisir ou mettre sous scellés le matériel ayant servi à commettre une infraction. Les sites pornographiques et érotiques sont de fréquents vecteurs de virus.
- **Consigne** : Les collaborateurs doivent savoir que les entités du Groupe collaborent systématiquement aux enquêtes diligentées par les autorités administratives ou judiciaires.

Situation de crise

- Toute situation dont les conséquences peuvent être graves pour une personne ou une entreprise, trouvant ses origines dans des faits exceptionnels (accident, catastrophe naturelle, agression, menace...) ou due à la répétition d'incidents provoquant un climat de tension. L'information relative à une situation de crise est une information sensible.
- **Risques** : Aggravation de la situation, rumeur, mise en cause erronée, faux témoignage.
- **Protection de l'information** : Les informations diffusées en situation de crise ne peuvent l'être que par des porte-parole dûment autorisés par le responsable de votre entité. Les collaborateurs doivent diriger les journalistes et enquêteurs vers les porte-parole officiels. Les collaborateurs interrogés par les autorités ne doivent rapporter que des faits, dont ils ont été les témoins directs, et s'abstenir de tout commentaire ou interprétation.
- **Protection de l'identité** : Ne rapporter que des faits et s'abstenir de mettre en cause des individus ou des institutions.
- **Protection du matériel / processus** : Éviter de modifier l'état des lieux en cas de catastrophe, d'accident ou d'agression afin de ne pas détruire des preuves ou des indices.
- **Consigne** : Les collaborateurs doivent connaître les noms des porte-parole en cas de situation de crise (ainsi que leurs coordonnées) ; ils sont désignés par les responsables des entités.

Smartphone

Voir "agenda électronique".

Spam

- E-mail envoyé à un très grand nombre de destinataires sans qu'il soit sollicité, on parle également de pourriel.
- **Risques** : Les spams encombrant les messageries et les serveurs, ils sont de fréquents vecteurs de virus. Ils sont le véhicule de publicités, mais surtout d'escroqueries : "phishing" (voir ce mot), de contrefaçons (médicaments, diplômes, montres, logiciel...), de jeux d'argent ou messages érotiques ou pornographiques (voir pornographie).
- **Protection de l'information** : Ne jamais transférer un spam, une lettre chaîne ou une pétition à un autre destinataire.
- **Protection de l'identité** : Les "spammeurs" cachent fréquemment leur identité.
- **Protection du matériel / processus** : Les spams sont de fréquents vecteurs de virus.
- **Consigne** : Les collaborateurs doivent apprendre à reconnaître les spams et savoir qu'il est interdit d'y répondre et d'ouvrir leurs pièces jointes.

Support

- Dans le contexte de la gestion des informations, le mot support désigne un objet qui contient des informations, par exemple : un CD, un DVD, une disquette, un badge magnétique, une “clé USB” (voir ce mot), un support non informatique (sur papier, film...).
- **Risques** : Vol, détérioration, classification inappropriée (voir ce mot), perte de “confidentialité” (voir ce mot).
- **Protection de l'information** : Voir “protection de l'identité” et “protection du matériel”.
- **Protection de l'identité** : Un support ne peut être communiqué qu'aux personnes autorisées à prendre connaissance des informations qu'il contient.
- **Protection du matériel** : Tenir les supports dans des endroits sûrs ou sécurisés. Ne pas les laisser sans surveillance sur votre bureau, dans un véhicule, une salle d'attente, un train, un avion...
- **Consigne** : Les collaborateurs doivent connaître les risques et règles de sécurité qui s'appliquent aux supports qu'ils utilisent.

Suppression de matériel

Voir “déplacement du matériel”.

Système d'information

- Ensemble des moyens (personnels, structures, procédures, équipements et matériels, données) nécessaires à la gestion (collecte, traitement, transmission, archivage...) des informations participant au fonctionnement d'une organisation.
- **Risques** : Perte de confidentialité, détérioration et indisponibilité de l'information.
- **Protection de l'information** : Les différents éléments du système ont des règles propres relatives à la protection de l'information et de leurs échanges. Ces règles sont rappelées dans les différentes rubriques du présent guide.
- **Protection de l'identité** : L'authentification (voir le mot “identifiant”) des utilisateurs du système d'information est la base de la protection de l'identité des utilisateurs d'un système d'information.
- **Protection du matériel / processus** : Les différents éléments d'un système d'information ont des règles propres relatives à la protection des matériels et processus.
- **Consigne** : Tout collaborateur doit connaître les règles relatives aux éléments du système d'information qu'il utilise.

Téléchargement

- C'est le transfert de données ou de programmes d'un ordinateur ou d'un “serveur” (voir ce mot) vers un autre ordinateur ou serveur. En théorie, on devrait distinguer la réception (“downloading”) de l'émission (“uploading”), mais en pratique le mot est principalement utilisé pour désigner la réception. C'est dans ce dernier sens que nous l'utilisons ici.
- **Risques** : Infraction aux droits d'auteur et copyrights, accès à des “sites interdits” (voir ce mot), “virus” (voir ce mot), incompatibilités avec certains éléments du “système d'information” (voir ce mot) de l'entreprise.
- **Protection de l'information** : Seuls sont autorisés les téléchargements correspondant à des besoins professionnels. Le téléchargement de logiciels (même gratuits), jeux, films et vidéos sont interdits (sauf autorisation du supérieur

hiérarchique et du support informatique (“support utilisateur”, “helpdesk”, “service desk”...) ainsi que les données en provenance de “sites interdits” (voir ce mot). Vérifier les droits d’auteurs (voir “propriété intellectuelle”) ou copyrights avant d’effectuer un téléchargement.

- **Protection de l’identité** : Ne pas se connecter à un site en dissimulant son identité de manière frauduleuse. Authentifier l’identité des sites auxquels on se connecte. Les collaborateurs qui utilisent des documents écrits par d’autres doivent citer leurs sources.
- **Protection du matériel / processus** : Ne pas télécharger de logiciel sans l’autorisation du support informatique (“support utilisateur”, “helpdesk”, “service desk”...).
- **Consigne** : Les collaborateurs doivent connaître les risques et les règles du téléchargement.

Téléphonie

- À l’origine la téléphonie était un système de transmission de la voix par des signaux électriques. Aujourd’hui la technologie permet de faire de la téléphonie sur les réseaux informatiques.
- **Risques** : Installation de dispositif d’écoute téléphonique. “Piratage” de l’appareil. Vol d’informations contenues dans le téléphone/smartphone (fixe ou portable). Usurpation d’identité. Phishing...
- **Protection de l’information** : Les informations ne sont réellement protégées que si elles sont cryptées. Les téléphones connectés aux réseaux sans fil (exemple : Bluetooth) sont particulièrement vulnérables. L’utilisation de ces appareils dans les lieux publics ne permet pas de garantir la confidentialité.
- **Protection de l’identité** : L’usurpation et la dissimulation d’identité sont difficiles à détecter lors d’une conversation téléphonique.
- **Protection du matériel** : Vol, perte ou détérioration suite à une surveillance défilante.
- **Consigne** : Les collaborateurs doivent être sensibilisés à l’importance des informations contenues dans leurs téléphones/smartphones (ex. : liste d’adresses) et au faible niveau de confidentialité de ce moyen de communication.

Télétravail

- Le télétravail est une forme d’organisation et/ou de réalisation du travail, utilisant les technologies de l’information et dans laquelle le travail est effectué hors des locaux de l’employeur de façon régulière.
- **Risques** : Tous les risques liés à l’utilisation de l’ordinateur et à celle de la télécommunication. Le travail à distance présente une difficulté pour la surveillance de l’utilisation des équipements nomades.
- **Protection de l’information** : La connexion à des réseaux non sécurisés (exemple : Wi-Fi public) peut augmenter les risques d’insécurité pour l’entreprise.
- **Protection de l’identité** : La procédure d’authentification des personnes travaillant à distance doit être définie, appliquée et contrôlée.
- **Protection du matériel / processus** : Le matériel situé à distance est sous la responsabilité de l’utilisateur, celui-ci doit avoir des instructions précises relatives à la protection du matériel en fonction de son utilisation et de son environnement.
- **Consigne** : Les règles relatives au télétravail doivent être définies en fonction des conditions d’utilisation et des réglementations locales.

Traçabilité

- C'est la faculté de retrouver l'historique de l'utilisation d'une information (qui a transmis à qui).
- **Risques** : L'absence de traçabilité ne permettrait pas de déterminer les responsabilités.
- **Protection de l'information** : La traçabilité permet de voir à quel moment (et par qui) une information est consultée ou modifiée.
- **Protection de l'identité** : La dissimulation d'identité par l'utilisateur fausse la traçabilité, mais il est très difficile de cacher l'identité de l'ordinateur ayant servi à une transaction informatique.
- **Protection du matériel** : Les matériels ayant servi à commettre une fraude peuvent être saisis par les autorités.
- **Consigne** : Les collaborateurs doivent savoir qu'il est facile de tracer les transferts d'information effectués au moyen de systèmes d'information, et que vouloir les fausser ou les dissimuler est une fraude.

Usage privé du matériel de l'entreprise (voir privé)

- Le Groupe n'a pas établi de règles générales pour l'usage privé des équipements des systèmes d'information. Après étude des incidences de la réglementation locale, les entités peuvent autoriser leurs collaborateurs à se servir modérément du téléphone/fax, de la messagerie ou d'Internet pour leurs propres besoins, ils peuvent également l'interdire.
- **Risques** : Violation de la vie privée des collaborateurs, utilisation inappropriée de l'Internet, engagement de la responsabilité du propriétaire de l'ordinateur (c'est-à-dire, de l'entreprise).
- **Protection de l'information** : Les règles de protections sont indépendantes de la nature de l'utilisation professionnelle ou privée des équipements.
- **Protection de l'identité** : L'utilisation du matériel de l'entreprise peut engager sa responsabilité, même quand le collaborateur l'utilise à des fins privées.
- **Protection du matériel** : Les règles de protections sont indépendantes de la nature de l'utilisation professionnelle ou privée des équipements.
- **Consigne** : Les collaborateurs doivent avoir des instructions qui leur indiquent si, et/ou dans quelles conditions, leur entité tolère qu'ils utilisent le téléphone/fax, la messagerie électronique et l'Internet.

Ver

- Logiciel malveillant transmissible d'ordinateur à ordinateur à l'insu des utilisateurs, via Internet, d'autres réseaux ou supports (CD, Clés USB). À la différence du virus, le ver ne nécessite pas d'action de l'utilisateur pour se propager. Son effet peut être différé.
- **Risques** : Destruction/détérioration des données et des programmes, piratage, usurpation d'identité.
- **Protection de l'information** : Seul compte la vigilance de l'utilisateur : ne pas ouvrir les pièces jointes, ne pas aller sur des sites non professionnels.
- **Protection de l'identité** : Seul compte la vigilance de l'utilisateur pour reconnaître les messages douteux et les sites douteux.
- **Protection du matériel /processus** : Les matériels doivent être équipés d'antivirus/anti-malware et se voir appliquer régulièrement les correctifs de sécurité en provenance des fournisseurs.

- **Consigne** : Informer les collaborateurs. Tout collaborateur qui soupçonne la contamination de son ordinateur doit avertir le support informatique (“support utilisateur”, “helpdesk”, “service desk”...), déconnecter son ordinateur du réseau pour éviter la diffusion d'un ver mais ne pas l'arrêter afin de faciliter les investigations ultérieures.

Verrouillage écran

- Le verrouillage de l'écran permet de bloquer l'accès aux informations disponibles à partir de l'ordinateur lorsque celui-ci est sous tension (par exemple, quand l'utilisateur s'en éloigne pour quelques instants).
- **Risques** : Ne pas verrouiller l'écran permettrait à un tiers de se servir de l'ordinateur en l'absence de son utilisateur légitime.
- **Protection de l'information** : Le verrouillage est recommandé afin de protéger les informations et leur échange (piratage, vol...).
- **Protection de l'identité** : Le verrouillage est recommandé afin d'éviter une utilisation frauduleuse sous l'identité de l'utilisateur légitime, le vol de données sensibles ou le concernant (“à caractère personnel”).
- **Consigne** : La méthode de verrouillage doit être connue des utilisateurs et automatisée tant que faire se peut.

Virus

- Logiciel malveillant, qui se transmet de façon invisible par les réseaux ou les supports d'information amovibles (exemple : clé USB), s'implante au sein des programmes en les parasitant, se duplique à l'insu des utilisateurs et produit ses effets dommageables quand le programme infecté est exécuté ou quand survient un événement donné.
- **Risques** : Destruction/détérioration des données et des programmes, piratage, usurpation d'identité.
- **Protection de l'information** : Seul compte la vigilance de l'utilisateur : ne pas ouvrir les pièces jointes de provenance inconnue ou douteuse, ne pas aller sur des sites non professionnels.
- **Protection de l'identité** : Seul compte la vigilance de l'utilisateur pour reconnaître les messages douteux et les sites douteux.
- **Protection du matériel / processus** : Les matériels doivent être équipés d'antivirus/anti-malware et se voir appliquer régulièrement les correctifs de sécurité en provenance des fournisseurs.
- **Consigne** : Informer les collaborateurs. Tout collaborateur qui soupçonne la contamination de son ordinateur doit avertir le support informatique (“support utilisateur”, “helpdesk”, “service desk”...), déconnecter son ordinateur du réseau pour éviter la diffusion d'un virus mais ne pas l'arrêter afin de faciliter les investigations ultérieures.

Visioconférence / vidéoconférence

- Réunion de personnes situées dans des lieux différents, unis par un réseau qui transmet l'image et le son (sans la vidéo, on parle alors de téléconférence). On dit aussi : vidéoconférence.
- **Risques** : Ecoute clandestine.
- **Protection de l'information** : Ne laisser aucun document dans les salles à l'issue de la vidéoconférence.
- **Protection du matériel / processus** : Les mesures techniques doivent être prises en vue d'empêcher une personne non clairement identifiée de rejoindre la visio/téléconférence sans intervention manuelle de l'organisateur.
- **Consigne** : Des notices d'emploi doivent être à la disposition des utilisateurs dans les salles équipées pour la vidéoconférence. Ces notices doivent renseigner les personnes en charge du support des matériels.

Vol

- Dans un système d'information, les vols peuvent concerner les informations, les matériels et les identités.
- **Risques** : Préjudice pour l'entreprise, le collaborateur voire des tiers.
- **Protection de l'information** : Les règles de la "classification" (voir ce mot) des informations ont pour objet d'apporter un niveau de protection approprié au niveau de confidentialité des informations.
- **Protection de l'identité** : Les procédures d'authentification (voir identifiant) ont pour objet de protéger des usurpations ou dissimulations d'identité.
- **Protection du matériel** : Pour éviter le vol de matériel, il existe des règles simples qui font appel à la vigilance des collaborateurs : surveillance et mise en lieu sûr des matériels, utilisation de systèmes de sécurité (exemple : câble de sécurité).
- **Consigne** : Les collaborateurs doivent connaître les méthodes de protection applicables aux matériels et processus qu'ils utilisent, même ceux qu'ils utilisent rarement.

Web

- Maillage de "serveurs" (voir ce mot) qui permet aux utilisateurs d'"Internet" (voir ce mot) de disposer de centaines de millions de pages d'informations (le Web est une application d'Internet, mais les mots sont aussi utilisés comme synonymes).
- **Risques** : Importation de virus, mise en relation potentielle avec des individus malfaisants (messages non sollicités, usurpation d'identité, escroquerie, vols, intrusion, espionnage, chantage...)
- **Protection de l'information** : Voir "Internet".
- **Protection de l'identité** : Ne donnez votre adresse e-mail qu'aux personnes en qui vous avez confiance, de nombreux sites revendent les adresses dont ils disposent (parfois aussi les informations vous concernant ou celles concernant votre entreprise). Veiller à protéger vos mots de passe.
- **Protection du matériel / processus** : Les réseaux sont le véhicule habituel des virus, vers, chevaux de Troie, spam, etc. Les réseaux des entreprises sont bien protégés contre ces risques, évitez de connecter votre équipement sur des réseaux non sécurisés (exemple : Wi-Fi public).
- **Consigne** : Les collaborateurs doivent connaître les risques liés à l'utilisation de l'Internet (Web, messagerie...). Ils doivent aussi savoir que l'entreprise a mis en place des outils pour surveiller l'usage des services Internet. Ces outils permettent notamment le contrôle des pratiques des utilisateurs (adresse des messages, sites visités, date et heure, durée d'utilisation).

Webcam

- Caméra numérique de petite taille branchée dans/sur un ordinateur, permettant de transmettre des images (et du son).
- **Risques** : Vol, perte de confidentialité, non-respect de la vie privée, risque réputationnel...
- **Protection de l'information** : Les informations diffusées par l'image et le son doivent avoir le même niveau de protection que celles diffusées par l'écrit.
- **Protection de l'identité** : Dans de nombreux pays, les images d'une personne sont des données à caractère personnel, elles sont soumises aux règles relatives à la protection de la vie privée. L'échange d'image au cours d'une conversation téléphonique entre des internautes permet la vérification d'identité.
- **Protection du matériel/ processus** : Les webcams amovibles peuvent être volées aisément.
- **Consigne** : Les collaborateurs ne doivent pas transmettre d'images susceptibles de représenter une infraction (atteinte à la vie privée, message diffamatoire, pornographie...).

Webcast

- Document audio ou vidéo diffusé sur Internet en live ou en différé. Un webcast n'est pas interactif.
- **Risques** : Tous les risques liés aux sites "Internet" (voir ce mot).
- **Protection de l'information** : La copie d'une partie ou de la totalité d'un webcast est soumise aux règles de protection de la propriété intellectuelle.
- **Consigne** : La consultation de webcasts doit avoir un motif professionnel. La reproduction de webcast peut être soumise à des règles de copyright.

Webinar

- Mot composé de Web et seminar : séminaire multimédia et interactif accessible sur le Web en direct ou en différé. Un Webinar comprend des images et du son, les participants peuvent poser des questions, soit en direct (voir "chat" ou "forum") quand la session se déroule en temps réel, soit par messagerie si elle se fait en différé. Les participants doivent s'inscrire au moyen d'un formulaire en ligne. Généralement, les Webinars sont payants, la confirmation de l'inscription est faite par Web et par e-mail, elle précise la procédure à suivre pour y participer.
- **Risques** : Virus, mais surtout risque d'indiscrétion, de diffamation, de propos/messages inappropriés, rumeur, perte de confidentialité, non-respect de la vie privée, dissimulation, voire usurpation d'identité. Irresponsabilité liée à l'anonymat, le cas échéant, espionnage industriel.
- **Protection de l'information** : Les participants doivent veiller à ne pas enfreindre les règles de confidentialité, ni échanger des propos qui pourraient constituer une infraction (vie privée, droits de la propriété intellectuelle, règles de la "concurrency" – voir ce mot –).
- **Protection de l'identité** : Ne participez qu'à des Webinars proposés par des institutions que vous connaissez. Soyez prudent sur vos commentaires, ne lésez ni vos intérêts, ni ceux de votre entreprise, ni même ceux d'un tiers, surtout dans le cas où vous ne connaissez pas les autres participants.
- **Consigne** : Les utilisateurs de Webinar doivent connaître leurs risques pour eux-mêmes, leur entreprise, voire des tiers.

Whistleblowing

Voir reporting des incidents.

ZIP

- Mode de compression de données afin de réduire leur place dans les mémoires (par exemple, pour accélérer leur transmission sur Internet). Il existe une fonction de codage du ZIP, ainsi seuls ceux qui ont le mot de passe peuvent connaître ce qu'il contient.
- **Risques** : Tous les risques habituels des fichiers et programmes. Risque d'in-discrétion si le mot de passe d'un ZIP codé n'est pas bien protégé.
- **Protection de l'information** : Ne pas transmettre le mot de passe par message-rie, mais par téléphone (ou SMS) afin d'augmenter le niveau de sécurité.
- **Protection de l'identité** : Ne pas dézipper un ZIP émis par un correspondant inconnu.
- **Protection du matériel / processus** : Comme les fichiers classiques, les ZIP peu-vent transporter des "virus" informatiques (voir ce mot).
- **Consigne** : Les collaborateurs qui utilisent des ZIP pour transmettre des infor-mations "diffusion restreinte" (voir "classification de l'information") doivent être capables de les coder et décoder. Contactez votre service de support informatique ("support utilisateur", "helpdesk", "service desk"...) pour connaître la procédure.

Ce document a été réalisé
par la Direction Ethique et Compliance
en collaboration avec
la Direction des Communications,
la Direction des Systèmes d'Information,
la Direction de la Sécurité
et la Direction des Ressources Humaines.

Les principes et conseils décrits dans le Code de Bonne Conduite doivent être appliqués dans le cadre des législations nationales propres à chaque pays.

Le vade-mecum a été réalisé à des fins didactiques.

Les traductions de ce document pouvant être sujettes à interprétation, seules les versions française et anglaise font office de référence.

Ce document a été imprimé sur un papier couché 100% recyclable et biodégradable, fabriqué et blanchi sans chlore dans des usines européennes certifiées ISO 9001 (qualité) et ISO 14001 (environnement). Les pâtes ayant servi à sa fabrication ont été obtenues à partir d'arbres provenant de forêts européennes certifiées PEFC, gage d'une gestion forestière durable. Ce papier ne contient pas de métaux lourds (taux inférieur à 100 ppm).

Edition juillet 2008