Charte d'utilisation du Système d'Information de la sarl COPYROOM

version 2015

CopyRoom sarl 28, rue de l'Erbonière 35510 Cesson-Sévigné

La présente « **Charte de bon usage du Système d'Information de la sarl CopyRoom** » définit les conditions d'utilisation des ressources informatiques des établissements, et des ressources informatiques externes accessibles via le réseau informatique des établissements, dans le respect des lois et règlements en vigueur.

La Charte inclut **Le système d'information de La sarl CopyRoom** notamment constitué des éléments suivants : ordinateurs (fixes ou portables), périphériques, assistants personnels, réseau informatique (serveurs, routeurs et connectique), photocopieurs, imprimantes, presses numériques, téléphones, logiciels, fichiers, données et bases de données, système de messagerie, intranet, extranet, abonnements à des services interactifs ; mais aussi les systèmes de nos clients accessibles par le réseau ou tout équipement informatique connecté à notre système d'information.

Elle précise les **droits et devoirs** de l'établissement, des personnels et des clients ou intervenants extérieurs ayant accès au système d'information, quel que soit leur statut. Elle rappelle les responsabilités des utilisateurs et les règles qui doivent régir leur usage professionnel et privé : « nul ne doit abuser des ressources informatiques mises à sa disposition par l'Entreprise pour l'accomplissement de ses missions ».

Elle précise les droits et devoirs spécifiques des responsables des systèmes informatiques (RSI), réseaux, applications et données qui bénéficient d'accès privilégiés au système d'information pour l'exercice de leur fonction.

Elle définit les devoirs spécifiques des responsables magasins concernant la gestion des accès octroyés aux clients et les procédures en cas de problèmes relevant de la responsabilité de la sarl CopyRoom.

Elle a pour vocation d'être diffusée à l'ensemble des personnels ainsi qu'aux utilisateurs occasionnels du système d'information de l'Entreprise, aussi la version papier et numérique seront accessibles dans les établissements dépendant de la sarl CopyRoom.

Dans les lieux où ces ressources peuvent être utilisées par des clients, par des personnes extérieures (techniciens ou stagiaires) ; dans le cybercafé Kennedy ou en connexion occasionnelle à CopyRoom et Artek Dynadoc), ou encore par accès Wifi, une version expurgée devra être affichée visiblement.

C'est « **un code de bonne conduite** », élément de base de la politique de sécurité du système d'information, présentant une valeur juridique, puisqu' annexée au règlement intérieur des établissements de la sarl CopyRoom.

Modifications du texte postérieures à son approbation au 1er mars 2015 :

-

Sommaire

Préambule

La présente charte définit les règles d'usages et de sécurité du système d'information que la sarl CopyRoom et l'utilisateur s'engagent à respecter. Elle précise les droits et devoirs de chacun.

Par « système d'information » s'entend l'ensemble des moyens matériels, logiciels, applications, bases de données, images, polices de caractère, documents et réseaux de télécommunications, pouvant être mis à disposition ou être accessibles à partir du système d'Information de la sarl CopyRoom. L'informatique nomade (clés USB, assistants personnels, ordinateurs portables, téléphones mobiles, etc...) est également un élément constitutif du système d'information qu'il soit connecté directement à un matériel ou via un réseau.

Le terme « client » désigne spécifiquement les personnes ou entités accédant aux ressources informatiques de la sarl CopyRoom ou permettant aux salariés de CopyRoom d'avoir accès à leur propre système ou données. Soit en libre-service pour un accès internet, soit par accès à des fichiers mis à disposition sur nos serveurs.

Le terme « utilisateur » désigne toute personne ayant accès, dans le cadre de l'exercice de son activité professionnelle, aux ressources du système d'information quel que soit son statut. Il s'agit notamment de :

- tout salarié quel que soit son statut, CDI ou CDD, intérimaire, stagiaire, dépendant de la sarl CopyRoom ;
- tout client accédant aux systèmes d'information, à titre onéreux ou gratuitement ;
- tout prestataire, technicien ou intervenant extérieur ayant un contrat avec la sarl CopyRoom.

Le bon fonctionnement du système d'information suppose le respect des dispositions législatives et réglementaires concernant la sécurité, la performance des traitements et la conservation des données.

Engagements de la sarl CopyRoom

La sarl CopyRoom met en œuvre toutes les mesures nécessaires pour assurer la sécurité du système d'information et la protection des utilisateurs.

La sarl CopyRoom facilite l'accès des utilisateurs aux ressources du système d'information. Les ressources mises à leur disposition sont prioritairement à usage professionnel mais la sarl CopyRoom est tenue de respecter l'utilisation ponctuelle du système d'information à titre privé.

Engagements de l'utilisateur et du client

L'utilisateur est responsable, en tout lieu, de l'usage qu'il fait du système d'information auquel il a accès ou lorsqu'il donne accès à des tiers. Il a une obligation de réserve et de confidentialité à l'égard des informations et documents auxquels il accède. Cette obligation implique le respect des règles d'éthique professionnelle et de déontologie.

En tout état de cause, l'utilisateur est soumis au respect des obligations résultant de son statut ou de son contrat.

Le client accepte les obligations de la Charte d'utilisation du Système d'Information liées à l'accès au réseau informatique, aux ressources ou à l'affichage des données.

L'acceptation tacite de la présente Charte d'utilisation du Système d'Information est réputée faite dès l'accès au matériel informatique, aux imprimantes ou aux photocopieurs et en cas de commande.

Le refus ou le non respect des modalités de la Charte d'utilisation du Système d'Information (ou de ses extraits à usage des clients), équivaut à la dénonciation du contrat nous liant avec le client. Aussi, celui-ci est seul responsable de ses agissements éventuels.

Article I. Champ d'application

Les règles d'usage et de sécurité figurant dans la présente charte s'appliquent :

- aux salariés ou stagiaires de la sarl CopyRoom sur nos propres systèmes d'information ou sur ceux de nos clients (par accès direct aux ressources, données du client, par utilisation du matériel informatique du client [ordinateur ou supports amovibles])
- aux utilisateurs clients ou intervenants extérieurs.

L'intrusion non autorisée dans le système d'information de la sarl CopyRoom peut être considérée comme une infraction (le fait d'accéder ou de se maintenir frauduleusement dans tout ou partie d'un système de traitement automatisé de données est punie de deux ans d'emprisonnement et de 30 000 Euros d'amende (Article 323-1 alinéa 1 du Code pénal).

L'annexe I encadre les missions du Responsable de Système d'Information.
L'annexe II encadre les responsabilités spécifiques des responsables de magasin.

Article II. Conditions d'utilisation du système d'information

Section II.1.0 Règles de base

II.1.0.1. Conditions d'accès

Le droit d'accès d'un utilisateur aux ressources informatiques est soumis à autorisation. Ce droit est **personnel** et **incessible**. Il disparaît dès que son utilisateur ne remplit plus les conditions qui lui ont autorisé l'accès.

Le Client a un usage temporaire du système d'information à des fins d'impression, de création de document en libre-service ou d'accès à internet. Ce droit d'accès disparait dès le départ des locaux.

II.1.0.2. Informations individuelles concernant l'utilisateur

Si l'accès au système d'information le nécessite, chaque utilisateur sera tenu de fournir des informations valides : adresses personnelle et/ou professionnelle, numéro de téléphone… permettant de le contacter en cas d'incident informatique. Il s'engage à notifier toute modification de ces informations.

II.1.0.3. Respect du caractère à priori confidentiel des informations

En l'absence d'une autorisation explicite, toute tentative d'accès à des informations détenues par d'autres utilisateurs est considérée comme illicite.

II.1.0.4. Sécurité de vos transactions et code d'accès

Les clients sont invités à saisir leur code bancaire ou leurs identifiants et mots de passe à l'abri des regards.

Section II.1.1 Mot de Passe

Le choix d'un mot de passe non trivial et son changement en cas de doute, notamment lorsqu'il a été utilisé à partir d'un poste connecté à un réseau extérieur non sécurisé, est une obligation pour l'utilisateur.

En cas d'absence, même temporaire, il est impératif que l'utilisateur verrouille l'accès au matériel qui lui est confié, dès lors que celui-ci contient des informations à caractère professionnel.

Un mot de passe peut être donné à certains utilisateurs pour accéder à des logiciels partagés (exemple ; logiciel de comptabilité) ou des codes bancaires pour effectuer des paiements

nécessaires à nos activités.

La confidentialité est impérative et aucun mot de passe ou code de toute nature ne doit être transmis sans autorisation du RSI ou de la Direction.

Section II.1.2 Antivirus

La sarl CopyRoom a mis en place des anti-virus sur son parc informatique.

Ces outils sont actualisés quotidiennement afin d'avoir la protection la plus efficace possible contre toute intrusion de virus. Les mises à jour se font automatiquement.

Il est formellement interdit à tout utilisateur de désinstaller l'anti-virus installé sur son PC ou d'en installer un autre sans l'accord du RSI.

Section II.1.3 Modifications matérielles ou logiciels

Le Client ne doit en aucun cas modifier l'environnement logiciel ou matériel auquel il a accès. En cas de message l'invitant à effectuer une mise à jour ou signalant un virus, le Client doit prévenir un salarié de la sarl CopyRoom afin de résoudre le problème.

L'Utilisateur ne doit pas modifier la configuration de son poste de travail et des autres équipements mis à sa disposition ou confié par des Clients, sans l'accord de l'administrateur du système d'information. En particulier :

- Il n'ajoute pas et ne retire pas de composant matériel (disque dur, carte réseau, etc…),
- Il n'installe pas de logiciels mais peut valider les mises à jour automatiques proposées des logiciels existants,
- Il ne tente pas de modifier ou de désactiver les mécanismes de protection (antivirus, paramétrage des mots de passe, installation des correctifs de sécurité, etc…)

En cas de besoin justifié, il s'adresse au RSI qui effectue les opérations nécessaires.

Section II.1.4 Accès aux ressources des Clients.

Les salariés de la sarl CopyRoom prennent en charge les impressions de fichiers à partir de supports amovibles physiques (clé USB, CD, DVD, ordinateur connecté, tablette etc…) et sont soumis à l'obligation de réserve et de confidentialité absolue sur les informations, données, photos, plans qu'ils auraient pu consulter ou imprimer pour le compte des Clients.

En cas d'accès aux ressources distantes des Clients, protégés ou non par mot de passe, les mêmes réserves de confidentialité sont appliquées. Les délais de réalisation des impressions ne commencent qu'une fois le téléchargement de la totalité des fichiers effectué.

En cas de prise de contrôle du matériel informatique distant du Client ou d'accès à un dossier par login/MDP, aucun fichier ne devra être téléchargé ou uploadé en dehors des fichiers nécessaires à l'impression ou à l'intervention demandée.

Section II.1.5 Corruption de fichiers, Dommages ou Perte de supports amovibles.

Tout support de données confié à un salarié ou un stagiaire de la sarl CopyRoom ou utilisé par le client sur notre parc informatique est réputé être une copie de travail du ou des fichier(s) original(aux).

Le bris de matériel, perte de support, ne donnera lieu qu'au remplacement dudit matériel ou au remboursement de sa valeur actualisée, le jour de la perte ou de la destruction du support.

La sarl CopyRoom décline toute responsabilité quant à l'infection éventuelle d'un support amovible (clé USB, disque dur, ordinateur, tablette, téléphone…) connecté à notre réseau ou à un poste informatique ou directement sur un photocopieur ou imprimante.

Tout dommage, qui pourrait être de notre responsabilité, concernant des fichiers infectés ou détruits, ne pourrait donner lieu à un quelconque dédommagement.

Tout dommage occasionné à un support physique (clé USB, disque dur, ordinateur, tablette, téléphone…) connecté directement sur nos matériels ou relié par réseau et endommagé suite à une surtension électrique ou tout problème relevant de notre responsabilité, ne donnera lieu qu'au remplacement dudit matériel ou au remboursement de sa valeur actualisée au jour du sinistre.

Section II.2.0 Utilisation professionnelle / privée

Le système d'information est destiné à des usages professionnels conformes aux missions de la sarl CopyRoom.

L'utilisation résiduelle du système d'information à titre privé est admise sous réserve qu'elle soit licite, non lucrative (interdiction total de la pratique des « jeux d'argent et de hasard en ligne ».) et raisonnable en termes de fréquence et de durée. Le surcoût qui en résulte doit demeurer négligeable au regard du coût global d'exploitation.

A ce titre, aucun abonnement à des services ou achat quelconque ne doit être réalisé par paiement effectué en différé sur la facture de l'opérateur télécom. (achat de « sonnerie » ou musique par exemple).

Il appartient à l'utilisateur de conserver ses données à caractère privé dans un espace prévu à cet effet en mentionnant le caractère privé sur la ressource de stockage (exemple : "PRIVE-nom-de-la-ressource"). Toute autre information est réputée à usage professionnel. La sauvegarde des données à caractère privé est effectuée avec les données professionnelles lorsqu'elles figurent sur un espace inclus dans le plan de sauvegardes automatiques de l'entité ; leur copie sur un support privé incombe à l'utilisateur. En l'absence de plan de sauvegardes automatiques, celles-ci doivent être effectuées par l'utilisateur. Il veillera alors à effectuer la copie régulière des données professionnelles sur un support fourni par l'entité et celle des données à caractère privé sur un support privé.

En cas de départ ou de décès, les données à caractère privé figurant sur le poste de travail ou tout autre matériel informatique mis à disposition par l'Entreprise, seront remises au salarié ou aux ayants droits, sur demande, au même titre que les affaires personnelles retrouvées sur le lieu de travail.

Section II.2.1 Utilisation de matériel personnel / professionnel

L'usage de ressources informatiques personnelles (un ordinateur, une tablette, un téléphone, un objet connecté, une clé USB,…) achetées sur des crédits personnels, lorsqu'elles sont utilisées pour accéder au système d'information de la sarl CopyRoom, ne doit pas remettre en cause ou affaiblir la sécurité en vigueur dans l'établissement.

Lorsque des données professionnelles (propriété de la sarl CopyRoom) sont présentes sur des ressources informatiques personnelles, il incombe à l'utilisateur de mettre tout en œuvre pour protéger ses données.

Le personnel, disposant de ressources informatiques professionnelles (un ordinateur, une tablette, un téléphone, un objet connecté, une clé USB,…) fournies par la sarl CopyRoom, accepte la politique de gestion de ses ressources mise en place par la sarl CopyRoom. A la fin de la mission lui ayant valu mise à disposition du matériel, l'utilisateur s'engage à le restituer à l'établissement.

Section II.3. Continuité de service : gestion des absences et des départs

II.3.0. Fichiers personnels et professionnels

Aux seules fins d'assurer la continuité de service, l'utilisateur informe sa hiérarchie des modalités permettant l'accès aux ressources mises spécifiquement à sa disposition. Il communiquera à son éventuel successeur la documentation technique électronique ou papier, les procédures mises en œuvre, les fichiers et données de toute nature permettant la continuité du travail.

L'utilisateur est responsable de son espace de données à caractère privé et il lui appartient de le détruire au moment de son départ. Les données professionnelles restent à la disposition de l'employeur et ne peuvent en aucun cas être altérées, modifiées ou supprimées. En tout état de cause les données non situées dans les répertoires « **privé** », « **personnel** » ou « **confidentiel** », sont considérées comme des données appartenant à l'établissement qui pourra en disposer.

Section II.4. Conformité aux règlements et lois en vigueur

II.4.1. Respect de la propriété intellectuelle

La sarl CopyRoom rappelle que l'utilisation des ressources informatiques implique le respect de ses droits de propriété intellectuelle ainsi que ceux de ses partenaires et plus généralement, de tout tiers titulaire de tels droits. En conséquence, chaque utilisateur doit :

- utiliser les logiciels dans les conditions des licences souscrites (notamment effectuer les éventuelles copies de manière strictement conforme aux dispositions prévues) ;
- ne pas reproduire, copier, diffuser, modifier, télécharger, uploader ou utiliser tout document numérique protégé par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits ;
- respecter le droit des marques.

II.4.2. Respect de la législation concernant le droit à la vie privée

Le droit à la vie privée, le droit à l'image et le droit de représentation impliquent qu'aucune image ou information relative à la vie privée d'autrui ne doit être mise en ligne ou utilisée sans l'autorisation de la personne intéressée.

II.4.3. Respect des clauses contractuelles des ressources électroniques

L'accès aux ressources documentaires électroniques (éditoriales ou illustratives : photos, dessins, vecteurs…) doit s'effectuer dans les conditions contractuelles des licences souscrites par la sarl CopyRoom.

II.4.4. Affichage de documents réservé aux personnes majeures

L'accès au contenu pornographique, violent, révisionniste ou aux fichiers illégaux est interdit.

L'affichage dans un lieu public d'images à caractère pornographique, violentes ou susceptible de heurter la sensibilité de clients du magasin est totalement interdit et tombe sous notre responsabilité. Aussi en cas d'infraction, la Direction avertira la gendarmerie et un dépôt de plainte sera susceptible d'être réalisé.

II.4.5. Respect des lois concernant la diffusion de l'information

L'utilisation des moyens informatiques mis à disposition par la sarl CopyRoom doit respecter la réglementation en vigueur. En particulier, la diffusion de messages diffamatoires ou injurieux, les provocations et apologies (crime, racisme, négationnisme, crime de guerre...), l'accès, la détention,

la diffusion d'images à caractère pédophile ou pornographique, la publication d'informations confidentielles sans autorisation préalable ou en violation du droit de la propriété intellectuelle sont strictement interdits.

II.4.6. Respect de la loi « informatique et libertés »

L'utilisateur est informé de la nécessité de respecter les dispositions légales en matière de traitement automatisé de données à caractère personnel, conformément à la loi n° 78-17 du 6 janvier 1978 dite «Informatique et Libertés» modifiée.

Les données à caractère personnel sont des informations qui permettent, sous quelque forme que ce soit, directement ou indirectement, l'identification des personnes physiques auxquelles elles s'appliquent.

Toutes les créations de fichiers comprenant ce type d'informations et demandes de traitement afférent, y compris lorsqu'elles résultent de croisement ou d'interconnexion de fichiers préexistants, devra en accomplir les formalités préalables auprès de la direction et informer les personnes concernées (type de données collectées, traitements, destinataires, etc.).

Par ailleurs, conformément aux dispositions de cette loi, chaque utilisateur dispose d'un droit d'accès et de rectification relatif à l'ensemble des données le concernant, y compris les données portant sur l'utilisation du système d'information. Ce droit s'exerce auprès du responsable du traitement.

Article III. Principes de sécurité à l'intention des salariés

Section III.1. Règles de sécurité applicables

La sarl CopyRoom met en œuvre les mécanismes de protection appropriés sur le système d'information mis à la disposition des utilisateurs.

L'utilisateur est informé que les mots de passe constituent une mesure de sécurité destinée à éviter toute utilisation malveillante ou abusive. Cette mesure ne confère pas aux outils informatiques protégés un caractère personnel.

Les niveaux d'accès ouverts à l'utilisateur sont définis en fonction de la mission qui lui est conférée. La sécurité du système d'information mis à sa disposition lui impose :

- de respecter les consignes de sécurité, notamment les règles relatives à la gestion des mots de passe ;
- de garder strictement confidentiels son (ou ses) mot(s) de passe et ne pas le(s) dévoiler à un tiers ;
- de respecter la gestion des accès, en particulier ne pas utiliser les mots de passe d'un autre utilisateur, ni chercher à les connaître ;
- d'utiliser des mots de passe différents pour accéder à des environnements différents (sites commerciaux, réseaux sociaux…) ou à des périmètres différents (utilisateur, administrateur, accès à une application spécifique…).

Si pour des raisons exceptionnelles et ponctuelles, un utilisateur se trouve dans l'obligation de communiquer son mot de passe personnel, il devra procéder, dès que possible, au changement de ce dernier ou en demander la modification à l'administrateur. Le bénéficiaire de la communication du mot de passe ne peut le communiquer à son tour à un tiers, ni l'utiliser en dehors de la circonstance exceptionnelle qui l'a conduit à en avoir connaissance. Sauf pour des raisons (cas de force majeure) de continuité de service et pour accès strictement limité aux données professionnelles.

La protection des ressources mises à la disposition de l'utilisateur nécessite l'application d'un certain nombre de règles élémentaires :

de la part de la sarl CopyRoom :

- veiller à ce que les ressources sensibles ne soient accessibles qu'aux personnes habilitées, en dehors des mesures d'organisation de la continuité du service mises en place (Cf. Section II.3) ;
- limiter l'accès aux seules ressources pour lesquelles l'utilisateur est expressément habilité ;

de la part de l'utilisateur :

- ne pas abuser des ressources informatiques auxquelles il a accès et être attentif à celles dont il a la responsabilité ;
- ne pas tenter d'accéder à des ressources du système d'information et aux communications entre tiers pour lesquelles il n'a pas reçu d'habilitation explicite ;
- ne pas rendre accessibles à des tiers les services qui lui sont offerts dans le cadre de son activité ;
- ne pas connecter aux réseaux locaux des équipements non autorisés par le RSI,
- ne pas installer, télécharger ou utiliser sur le matériel de la sarl CopyRoom, des données, logiciels ou progiciels dont les droits de licence n'ont pas été acquittés, ou ne provenant pas de sites dignes de confiance ;
- ne pas déposer des données professionnelles (pour lesquelles a été identifié un besoin direct ou indirect de confidentialité) sur un serveur externe et/ou ouvert au grand public, dans « le cloud » ou sur le poste de travail d'un autre utilisateur sans analyse de risques préalable réalisée en concertation avec le RSI ;
- se conformer aux dispositifs mis en place par la sarl CopyRoom pour lutter contre les virus et les attaques par programmes informatiques ;
- ne pas nuire volontairement au bon fonctionnement des ressources informatiques et des réseaux par des manipulations anormales du matériel ou par l'introduction de logiciels malveillants ou intrusifs (virus, chevaux de Troie, bombes logiques, outils d'intrusion...). En cas d'usage contrevenant à cette interdiction pour des raisons justifiées, une demande préalable devra être formulée auprès du RSI ;
- assurer la protection des informations sensibles et ne pas les transporter sans protection (telle qu'un chiffrement) sur des supports mobiles (ordinateurs portables, clés USB, disques externes, etc.) ;
- ne pas quitter son poste de travail, a fortiori un ordinateur en libre-service, sans se déconnecter ou verrouiller sa session par un mot de passe.

Section III.2. Devoirs de signalement et d'information

L'utilisateur doit avertir le RSI dans les meilleurs délais en cas de découverte d'une anomalie affectant le système d'information, notamment une intrusion ou une tentative d'accès illicite à son propre compte.

Section III.3. Mesures de contrôle de la sécurité

L'utilisateur est informé :

- que pour effectuer la maintenance corrective, curative ou évolutive, la sarl CopyRoom se réserve la possibilité de réaliser des interventions (le cas échéant à distance) sur les ressources mises à sa disposition ;
- qu'une intervention à distance sur le poste de travail de l'utilisateur est précédée d'une information de ce dernier ;
- que toute donnée bloquante pour le système ou générant une difficulté technique d'acheminement à son destinataire, sera isolée ; le cas échéant supprimée.

La sarl CopyRoom informe l'utilisateur que le système d'information peut donner lieu à une surveillance et un contrôle à des fins statistiques, de traçabilité, d'optimisation, de sécurité ou de détection des abus, dans le respect de la législation applicable.

Les personnels chargés des opérations de contrôle du système d'information sont soumis à l'obligation de discrétion. En revanche, ils doivent communiquer toutes informations mettant en cause le bon fonctionnement technique des applications ou leur sécurité, ou aux autorités compétentes si elles tombent dans le champ de l'article 40 alinéa 2 du code de procédure pénale.

Article IV. Communication électronique

Section IV.1. Messagerie électronique

La messagerie est un moyen de communication ouvert à des usages professionnels contribuant aux missions de l'entreprise.

IV.1.1. Adresses électroniques

Une adresse électronique, fonctionnelle ou organisationnelle, peut être mise en place pour un utilisateur ou un groupe d'utilisateurs pour les besoins de la sarl CopyRoom.

L'aspect nominatif de l'adresse électronique constitue le simple prolongement de l'adresse administrative : il ne retire en rien le caractère professionnel de la messagerie.

La gestion d'adresses électroniques ou de toute base de données (base des clients ou prospects par exemple), relève de la responsabilité exclusive de la sarl CopyRoom : ces listes ne peuvent être utilisées sans autorisation explicite.

Le filtrage des adresses d'envoi, du sujet ou du contenu du mail, est assuré par un antispam. Il convient à l'utilisateur de créer des filtres permettant l'arrivée effective des mails de ses contacts.

IV.1.2. Contenu des messages électroniques

Tout message est réputé professionnel sauf s'il comporte une mention particulière et explicite indiquant son caractère privé ou s'il est stocké dans un espace privé de données.

Pour préserver le bon fonctionnement des services, des limitations peuvent être mises en place.

Les messages comportant des contenus à caractère illicite quelle qu'en soit la nature sont interdits.

L'utilisateur doit veiller à ce que la taille des messages reste raisonnable et à ce que leur diffusion soit limitée aux seuls destinataires concernés afin d'éviter les envois de messages en masse, l'encombrement inutile de la messagerie ainsi qu'une dégradation ou saturation du service.

IV.1.3. Statut et valeur juridique des messages

Les messages électroniques échangés avec des tiers peuvent, au plan juridique, former un contrat, sous réserve du respect des conditions fixées par les articles 1369-1 à 1369-11 du code civil.

L'utilisateur doit, en conséquence, être vigilant sur la nature des messages électroniques qu'il échange au même titre que pour les courriers traditionnels.

IV.1.4. Stockage et « archivage » des messages

Les serveurs de messagerie effectuent la sauvegarde temporaire des boîtes à lettres en prévention des erreurs de manipulation des utilisateurs et des pannes des équipements. Cette sauvegarde ne garantit pas le recouvrement de l'ensemble des messages reçus (exemple : message détruit entre le moment de son arrivée et celui de sa sauvegarde). Les utilisateurs devront pouvoir effectuer la restauration ou la supression des messages stockés.

Les supports numériques ne garantissent pas l'archivage de manière certaine. Chaque utilisateur doit procéder à l'impression des messages pouvant être indispensables ou simplement utiles en tant qu'éléments de preuve.

Section IV.2. Internet

La sarl CopyRoom offre un accès à l'intranet de l'établissement ainsi qu'à l'ensemble du réseau Internet pour un usage dédié à la réalisation de ses activités professionnelles. Une utilisation résiduelle privée, telle que définie en section II.2, est admise. Il est rappelé qu'Internet est soumis à l'ensemble des règles de droit en vigueur.

IV.2.1. Publication sur les sites internet et intranet de la sarl CopyRoom

Toute publication de pages d'information sur les sites internet ou intranet de la sarl CopyRoom doit être validée par un responsable de site ou responsable de publication.

Sauf autorisation explicite de l'établissement, il est interdit d'employer les chartes graphiques et les logos des sites internet des entités rattachées à la sarl CopyRoom (ou tout autre apparence approchante) hors des serveurs de ces domaines « CopyRoom.fr Kennedy-photocopie.com artekrepro.fr dynadoc.fr prix-devis-tarif.com ».

Aucune information relative aux spécificités du Système d'Information de la sarl CopyRoom ne doit être publiée sans autorisation préalable.

IV.2.2. Sécurité

L'accès Internet n'est autorisé qu'au travers des dispositifs de sécurité mis en place par la sarl CopyRoom.

La sarl CopyRoom se réserve le droit de filtrer ou d'interdire l'accès à certains sites, de procéder au contrôle à priori ou à posteriori des sites visités.

L'utilisateur est informé des risques et limites inhérents à l'utilisation d'Internet par le biais de la présente charte, de notes spécifiques et d'actions de formations.

IV.2.3. Téléchargements et « mises en ligne »

Tout téléchargement ou upload de textes, de sons, d'images, de vidéos, de logiciels et tous autres documents, sur Internet ou vers nos unités de stockage, doit s'effectuer dans le respect des règlements et lois en vigueur (Cf. sous-section II.4).

La sarl CopyRoom se réserve le droit de limiter le téléchargement de certains fichiers pouvant se révéler volumineux ou présenter un risque pour la sécurité du système d'information (virus susceptibles d'altérer le bon fonctionnement du système d'information de la sarl CopyRoom, codes malveillants, programmes espions, etc…).

Article V. Journalisation des accès

La sarl CopyRoom est dans l'obligation légale de mettre en place un système de journalisation des accès Internet, de la messagerie et des caractéristiques des données échangées. La gestion des journaux informatiques (finalités, contenus, traitements, droits d'accès, destinataires, délais de conservation…) est conforme aux règles énoncées dans un document spécifique et à leur déclaration auprès de la Commission Nationale de l'Informatique et des Libertés en application de la loi n° 78-17 du 6 janvier 1978 modifiée.

Article VI. Limitation des usages et sanctions des abus

En cas de non-respect des règles définies dans la présente charte, la Direction pourra, sans préjuger des poursuites ou procédures de sanctions pouvant être engagées à l'encontre des personnels, limiter les usages par mesure conservatoire.

Tout abus dans l'utilisation des ressources mises à la disposition de l'utilisateur à des fins extra-professionnelles est passible de sanctions. Outre les sanctions pénales prévues par le code pénal (amendes et/ou emprisonnement), les salariés encourent des sanctions disciplinaires conformément aux dispositions législatives, règlementaires et statutaires en vigueur.

Article VII. Entrée en vigueur de la charte

La présente charte a été approuvée le 1er mars 2015 par le gérant Jean-Michel Blatry et le Responsable de la Sécurité Informatique, Julien Dubois.

Annexe I. Responsables/administrateurs de Système d'Information (RSI)

La présente annexe a pour objet de formaliser les règles de déontologie et de sécurité s'appliquant spécifiquement aux Responsables du système d'information de la sarl CopyRoom.

Cette annexe est indissociable de la « **Charte de bon usage du système d'information de la sarl CopyRoom** » qu'elle complète en précisant les droits et devoirs des RSI.

Annexe I.1. Définition et mission d'un Responsable / administrateur de système d'information (RSI)

Le terme « administrateur » désigne toute personne, employée ou non par la sarl CopyRoom, chargée explicitement du bon fonctionnement et de la sécurité de ressources informatiques faisant partie du système d'information des établissements de la sarl CopyRoom et qui est placée sous sa responsabilité.

Dans le but d'assurer la disponibilité, l'intégrité, la confidentialité et la journalisation des accès aux données, réseaux, systèmes et applications dont il a la responsabilité, l'administrateur met en œuvre les mesures SSI (Sécurité du Système d'Information) nécessaires. Leur mise en place est conditionnée par la définition des objectifs de sécurité fixés par la Direction, juridiquement responsable en cas d'incident, et par les moyens pouvant y être affectés.

Annexe I.2. L'administrateur et la sécurité du système d'information

Dans le cadre de l'exploitation, la maintenance et le suivi de l'utilisation des ressources informatiques de son périmètre d'activité, l'administrateur du système d'information est amené à effectuer des actions spécifiques lui permettant d'assurer la continuité de service. Ces actions lui donnent potentiellement accès à l'ensemble des « données utilisateurs ». Habituellement, les données auxquelles il accède se limitent aux données issues de la métrologie, de la surveillance, de l'audit des réseaux et systèmes et/ou aux données nécessaires aux diagnostics de dysfonctionnements et aux recherches de malveillances.

En cas d'incident, des investigations peuvent cependant l'amener à prendre indirectement connaissance d'informations de nature confidentielle, si ces données ne sont pas protégées par un mécanisme de chiffrement ; il est alors soumis au devoir de confidentialité (voir Annexe I.3)

Les équipements, systèmes, applications, ainsi que les outils dont l'administrateur fait usage dans l'exercice de sa fonction, sont exclusivement professionnels et autorisés par la sarl CopyRoom.

L'administrateur met en œuvre une procédure de gestion des accès aux ressources informatiques ainsi que des mécanismes d'authentification.

Une trace logique (« Logs » : date et heure, description des événements…) de tous les incidents de sécurité survenus dans son périmètre d'activité doit être conservée.

Enfin, l'administrateur est responsable de la mise à jour des systèmes, applications et dispositifs de sécurité, (nouvelles versions, correctifs de sécurité,…) dont il a la charge. Ces mises à jour doivent être effectuées avec discernement ; la maturité de la dernière version est à prendre en compte avant tout changement majeur. Il est chargé de la documentation des procédures qu'il met en place pour l'administration des services vitaux.

Annexe I.3. Droits et devoirs spécifiques

L'administrateur est soumis à la présente « Charte de bon usage ». Il doit, d'une manière générale, respecter les règles d'éthique professionnelle, de déontologie, l'obligation de réserve ainsi que le devoir de discrétion.

Cependant, pour exercer son rôle au sein du système d'information de l'établissement, il a des droits et des devoirs spécifiques.

Dans le cadre de ses missions, l'administrateur a le droit :

- d'être informé des implications légales de son travail, y compris des risques qu'il encourt dans le cas où un utilisateur du système dont il a la charge commettrait une action répréhensible ;
- de prendre toute disposition nécessaire au bon fonctionnement des ressources informatiques dont il a la charge ;
- d'établir des procédures de surveillance des données, réseaux, systèmes et applications, afin de déceler les anomalies, ayant préalablement informé les utilisateurs ;
- d'accéder à toute information utile (y compris les fichiers de journalisation) à des fins de diagnostic et d'administration du système, en respectant ses engagements de confidentialité et de non divulgation de ces informations.

Dans le cadre de ses missions, l'administrateur a le devoir :

- d'améliorer en permanence la qualité de service et de la sécurité, dans l'intérêt de l'entité, de l'établissement et des utilisateurs ;
- de respecter la plus stricte confidentialité des mots de passe des utilisateurs dont il aurait pu avoir connaissance ;
- de garder strictement confidentiel son mot de passe « administrateur » sous réserve des dispositions prévues à la Section II.3 (continuité de service) ;
- de respecter la confidentialité absolue des informations privées ou à caractère personnel dont il a eu connaissance dans le cadre de l'exercice de sa mission, ces informations ne pouvant légalement être communiquées qu'aux personnes appartenant à la « chaîne fonctionnelle de sécurité du système d'information » de la sarl CopyRoom et aux autorités judiciaires ;
- de veiller à ce que les tiers non-autorisés n'aient pas connaissance d'informations privées ou à caractère personnel ;
- d'organiser la continuité des services numériques (équipements, documentation, accès…) afin de minimiser les conséquences de son éventuelle indisponibilité ;
- de mettre en œuvre un système de journalisation des accès aux ressources informatiques («logs») conforme à la « Politique de Gestion des Journaux Informatiques « de la sarl CopyRoom ;
- d'examiner régulièrement ces journaux pour une détection précoce des dysfonctionnements et incidents de sécurité ;
- de veiller à la déclaration des traitements automatisés d'informations nominatives auprès de la CNIL, conformément à la réglementation en vigueur ;
- de refuser de répondre à une demande qui aurait pour conséquence de lui faire commettre une infraction (droit à la vie privée, droit au secret de la correspondance, loi Informatique et Libertés, etc…), en dehors des requêtes des autorités judiciaires ;
- d'agir au plus tôt lorsqu'il a connaissance d'actions illégales ou de données illicites (Cf. Section II.4) sur les équipements, systèmes ou applications dont il a la responsabilité en isolant le composant en cause (fichier, serveur…), et en informant la Direction ;
- de veiller au respect, par les utilisateurs, de la présente « Charte de bon usage » et des consignes de sécurité.

Annexe I.4. Alertes internes à l'entité.

L'administrateur doit tenir informée la Direction des choix et difficultés techniques liées à l'exercice de sa fonction : propositions d'amélioration des services et de la sécurité, conseil en ingénierie informatique, budget en accord avec les objectifs, besoins de formations, etc.

L'administrateur doit tenir informée la Direction des incidents de sécurité et vulnérabilités du système d'information rencontrés dans l'exercice de sa mission : tentatives d'intrusion, virus détectés, matériels obsolètes, saturation de ressources informatiques, plan de reprise/continuité d'activité non opérationnelle, etc… D'une manière générale, il doit signaler tout événement, règle de sécurité violée, charte de bon usage non respectée, et toutes autres activités non conformes pouvant avoir un impact légal ou réglementaire ou bien induisant un risque (technique, juridique, financier, image de marque…) non négligeable pour l'entité.

Annexe I.5. Chaîne d'alerte de la sarl CopyRoom

L'administrateur doit mettre en œuvre les mesures issues de la chaîne d'alerte de la sécurité informatique de l'établissement. En particulier, il lui incombe de :

- prendre toutes mesures nécessaires suite aux alertes d'un responsable magasin et aux consignes de l'Entreprise lorsque les ressources informatiques dont il a la responsabilité sont concernées ;
- fournir à la Direction les informations nécessaires à l'évaluation de la gravité d'un incident de sécurité et, le cas échéant, apporter les éléments nécessaires à la constitution du dossier pour suite à donner ;
- coopérer à la résolution des incidents et se conformer aux directives du RSI, en fonction de la nature et de la gravité de l'incident ;
- répondre aux sollicitations des autorités judiciaires (généralement relayées par un Officier de Police Judicaire) en relation avec la Direction de l'établissement.

Annexe I.6. Information des utilisateurs

La mise à disposition de ressources informatiques s'accompagne nécessairement d'une information auprès des utilisateurs concernés. L'administrateur est donc tenu de :

- porter à leur connaissance les informations et les traitements auxquels il a accès de par sa fonction ;
- les informer, dans la mesure du possible, de toute intervention nécessaire, susceptible de perturber ou d'interrompre l'utilisation habituelle des ressources informatiques ;
- les informer des derniers incidents ayant perturbé ou interrompu l'utilisation habituelle des ressources informatiques ;
- les informer de toute opération conduisant à accéder à leur poste informatique, et du motif justifiant cette intervention (sauf lorsque la discrétion des opérations est imposée par les autorités judiciaires) ;
- leur communiquer les règles de bon usage du système d'information de l'Entreprise et du réseau, les sensibiliser aux problèmes de sécurité informatique, leur faire connaître les consignes techniques de sécurité.

Annexe I.7. Mesures préventives à mettre en œuvre sur le matériel informatique en libre-service.

Plusieurs mesures préventives doivent être mise en œuvre pour éviter toute intrusion sur les Pc, sur le réseau et le serveur de document.

- **Matériel en libre-service :**

Le client doit pouvoir utiliser les logiciels de bureautique, accéder à internet et effectuer les impressions sans être interrompu dans le travail courant et en toute sécurité pour ses documents.

- L'antivirus doit être activé avec mise à jour automatique de bases de virus.
- En cas de connexion d'une clé USB ou disque dur, l'antivirus doit scanner le support et détecter les virus ou malwares éventuels.
- Le client ne doit pas pouvoir installer un logiciel sur le poste sans saisie du login/mdp.
- Le client ne doit pas pouvoir accéder au réseau ou au serveur de document sauf sur les dossiers spécifiques (scan de document – partage limité – autre dossier à définir)
- L'accès aux sites pornographiques, pédophiles, révisionnistes, warez doit être interdite.
- Les mises à jour logicielles doivent être réalisées régulièrement par le RSI ou le responsable magasin.

- **L'accès au serveur :**

Le serveur ne doit pas être accessible par le client, tout comme le serveur de document à partir d'un PC en libre-service.

- Interdire la connexion montante du PC vers le serveur sans saisie de login/mdp.

Annexe I.8. Mesures préventives à mettre en œuvre pour l'accès à des documents accessibles par un client identifié.

- **Mise à disposition d'un dossier accessible à partir de l'extérieur pour les clients identifiés :**

Pour le partage de documents, nous pouvons mettre à disposition un espace privatif pour nos clients. Celui-ci est protégé par login/mdp imposé par le RSI.

- Vérifier la non-intrusion au reste du réseau après connexion pour chaque login/MDP communiqué à un client.
- Lui transférer les login/MDP avec la Charte d'utilisation au Système Informatique en demandant le retour de la feuille d'engagement.

- **Accessibilité d'un fichier ou d'un dossier compressé :**

Formation des responsables de magasins et des salariés pour la mise à disposition d'un fichier unique ou d'un dossier zippé, il faudra qu'ils puissent créer :

- Un dossier spécifique de dépôt des fichiers pour les clients,
- Un lien direct sur l'espace de partage du serveur,
- Envoi du lien au client par mail avec accusé de réception pour s'assurer de la bonne réception du mail.

Annexe I.9. Journalisation des flux.

- **Création de journaux système sur les serveurs :**

Les journaux systèmes produits à mettre en place sur nos serveurs informatiques permettront la surveillance du contrôle d'accès à nos systèmes et réseaux. Ils permettront de faciliter les investigations ultérieures, et sont en outre également exigés dans le cadre de la collecte de preuve par les autorités juridiques compétentes.

Les journaux systèmes qui enregistrent les activités des utilisateurs, les exceptions et les événements liés à la sécurité doivent être produits et conservés pendant 1 an maximum pour surveiller l'exploitation du système.

Il est important de protéger le dossier qui conserve les informations journalisées contre les accès non autorisés ou des actes de malveillances qui pourraient s'opposer au maintien de la preuve.

Annexe I.10. Mesures conservatoires

Le non-respect, délibéré et en connaissance de cause, par un administrateur des règles spécifiques définies dans la présente annexe peut entraîner des sanctions de natures disciplinaires et/ou pénales.

Annexe II. Responsabilités spécifiques des responsables de magasins

La présente annexe a pour objet de formaliser les règles de déontologie et de sécurité s'appliquant spécifiquement aux Responsables des magasins de la sarl CopyRoom.

Cette annexe est indissociable de la « **Charte de bon usage du système d'information de la sarl CopyRoom** » qu'elle complète en précisant les droits et devoirs des responsables de magasins.

Annexe II.1. Définition et mission d'un Responsable de magasin en matière de régulation de l'accès au Système d'Information

Le responsable d'un magasin de la sarl CopyRoom doit mettre en œuvre les modalités d'accès au Système d'Information pour nos clients et intervenir lorsque la responsabilité de la sarl CopyRoom.

La responsabilité de la sarl CopyRoom est engagée lorsqu'un client :

- Se connecte à un matériel pour y réaliser une impression ;
- Effectue des mises en page sur un ordinateur en libre-service ;
- Affiche des documents illicites à la vue des autres clients du magasin ;
- Se connecte à Internet pour y effectuer des actions répréhensibles telles que :
    - Envoi de mail en masse,
    - Téléchargement ou upload de fichiers, données, musiques, logiciels illicites ou dont il ne dispose pas des droits d'usage,
    - Envoi de liens, documents, mails, messages, ou les posts sur médias sociaux,
        - diffamatoires ou injurieux,
        - provocants ou faisant l'apologie du crime, racisme, négationnisme, crimes de guerre...,
        - (1) permettant l'accès, la détention, la diffusion d'images à caractère pédophile ou pornographique à destination de mineurs, la publication d'informations confidentielles…
- Se connecte à internet pour se livrer à des actions répréhensibles :
    - Gestion de sites prohibés, tels que (voir (1))
    - Collecte ou transmission de fonds pour des organisations terroristes,
    - Usurpation d'identité, achats frauduleux…

Annexe II.2. En cas de détection de virus sur le support du client

Le responsable du magasin indique au client :

- Le virus ne doit pas se propager : le client ne doit pas « tester » qu'autres postes pour ouvrir sa clé s'il constate une absence de données ou qu'un virus soit détecté par notre antivirus,
- Que l'utilisation de nos matériels implique l'adhésion tacite à la Charte d'utilisation du Système d'Information de la sarl CopyRoom.
- Que nos matériels sont protégés par un anti-virus quotidiennement mis à jour,
- Que le virus provient éventuellement d'un ordinateur infecté, probablement le sien ou celui de l'université (s'il est étudiant),

- Si le client insiste : notre responsabilité se limite au remplacement de son support après vérification par un centre technique.

- Nous pouvons tenter de récupérer les données de son support après audit du virus s'il est possible d'en connaitre le nom. Alerter le RSI.

Annexe II.3. En cas destruction ou perte du support du client

Le responsable du magasin indique au client :
- Que l'utilisation de nos matériels implique l'adhésion tacite à la Charte d'utilisation du Système d'Information de la sarl CopyRoom.
- Que notre responsabilité se limite au remplacement de son support après vérification par un centre technique s'il a été endommagé.

Annexe II.4. Intrusion d'un logiciel.

Difficile de se rendre compte de l'utilisation abusive de nos postes
Plusieurs cas de figures peuvent survenir :

- Si le client installe volontairement un logiciel malveillant (cheval de troie, keylooger…) sur le matériel ou si celui-ci est installé au « lancement du document à imprimer » :

  Le responsable du magasin :
  - Indique au client que l'utilisation de nos matériels implique l'adhésion tacite à la Charte d'utilisation du Système d'Information de la sarl CopyRoom,
  - Demande au client de ne pas essayer sur d'autres postes,
  - Restore une version « propre » du système d'exploitation si le virus ne peut pas être ôté ou n'est pas éradiqué par l'antivirus.

  Le RSI devra veiller à ce que l'installation d'un programme soit uniquement possible après saisie du login / mot de passe du matériel.

Annexe II.5. En cas d'affichage à la vue de personne mineure d'un contenu à caractère pornographique.

Le responsable du magasin :
- Effectue une copie d'écran immédiate qui restera sur l'ordinateur,
- Procède à l'extinction de l'écran mais pas de l'ordinateur pour garder la preuve du l'affichage,

Le responsable du magasin indique au client :
- Que l'utilisation de nos matériels implique l'adhésion tacite à la Charte d'utilisation du Système d'Information de la sarl CopyRoom,
- Que l'affichage d'un contenu pornographique à un mineur constitue un acte répréhensible,
- Que nous souhaitons obtenir son identité sinon nous prévenons les autorités.)Si le responsable légal porte plainte, nous aurons des éléments à communiquer).

- En cas de refus, prévenir la Direction qui avertira éventuellement la gendarmerie.

- Contacter le RSI pour qu'il effectue une copie de la vidéosurveillance du magasin.

Annexe II.6. En cas d'affichage d'images à caractère pédophile.

Le responsable du magasin :
- Effectue une copie d'écran immédiate qui restera sur l'ordinateur,
- Procède à l'extinction de l'écran mais pas de l'ordinateur pour garder la preuve du l'affichage,
- Conserve l'identité des témoins.

Le responsable du magasin indique au client :
- Que l'utilisation de nos matériels implique l'adhésion tacite à la Charte d'utilisation du Système d'Information de la sarl CopyRoom,

- Que l'affichage d'un contenu pédophile constitue un acte répréhensible,
- Que nous souhaitons obtenir son identité sinon nous prévenons les autorités. (Si une personne porte plainte, nous aurons des éléments à communiquer si nous avons l'identité)

- Prévenir la Direction qui prendra les mesures éventuelles (dépôt de plainte auprès de la gendarmerie).
- Contacter le RSI pour qu'il effectue une copie de la vidéosurveillance du magasin.
-

Annexe II.7. En cas d'accès à des sites non autorisés.

L'écran affiche « Site non accessible »

- Avertir le client que le site n'est pas accessible en raison du blocage par le routeur des sites malveillants ou interdits en cycbercafé.

Annexe III. Glossaire

Ci-dessous, l'explicitation des sigles, acronymes, et termes :

Antispams : logiciels conçus pour détecter et éliminer les spams. Basés sur diverses méthodes de reconnaissance (analyse de l'entête, analyse du contenu, réputation et/ou comportement du relais de messagerie, etc…), ils sont mis en œuvre sur les passerelles de messagerie et/ou les postes de travail.

Antivirus : logiciels conçus pour détecter et éliminer des codes malveillants tels que virus, vers, chevaux de Troie. Basés sur une recherche de « signatures » (partie de code spécifique), ils sont mis en œuvre sur les passerelles de messagerie et/ou les postes de travail.

Bombe logique : logiciel destiné à altérer ou détruire partiellement ou totalement un système informatique (déclenchement sur date ou autre événement).

Canular informatique (**Hoax** en anglais) **:** forme de spam dont la diffusion se fait de proche en proche (chaîne de lettres par exemple). La forme de propagation (destinataire sollicité pour faire suivre vers ses correspondants habituels, contenu alarmant mais plausible…) endort la vigilance des destinataires et rend sa détection difficile par les antispams.

Cheval de Troie (**Trojan horse** en anglais) **:** code malveillant généralement intégré à un programme légitime pour effectuer une action nuisible. Beaucoup comportent une « porte dérobée » (**backdoor** en anglais) permettant une prise de contrôle à distance de l'ordinateur.

CIL (Correspondant Informatique et Libertés) **:** le CIL veille à la bonne application de la loi informatique et libertés dans l'établissement ; il doit établir et maintenir un registre des traitements mis en œuvre dans l'établissement.

CNIL (Commission Nationale de l'Informatique et des Libertés) **:** autorité administrative indépendante créée par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Hameçonnage (**Phishing** en anglais) **:** sollicitation frauduleuse d'extorsion de mot de passe (ou autre information personnelle « sensible » telle que numéro de Carte Bleue) par messagerie ou via un site web contrefait.

Journaux informatiques (**traces** ou **logs**) **:** données de connexion pouvant aider à retracer les attaques, les activités inhabituelles ou inappropriées qu'elles soient d'origine interne ou externe.

Malware (**code malveillant** en français) **:** mot générique pour désigner un logiciel nuisible pour le système d'information (virus, ver, cheval de Troie, porte dérobée, logiciel espion, etc…).

PSSI (Politique de Sécurité du Système d'Information) **:** ensemble formalisé dans un document applicable, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection du système d'information de l'établissement.

RSI (Responsable de la sécurité du Système d'Information) **:** il a pour mission l'élaboration et la mise en mise en œuvre, en relation avec la Direction, de la politique de sécurité du système d'information de l'établissement.

SI (Système d'Information) **:** ensemble organisé de ressources (personnels, applications et équipements informatiques, données, procédures…) nécessaire au traitement de l'information, dans le cadre d'objectifs définis au niveau de la stratégie de l'établissement.

Spam (**pollupostage** ou **pourriel** en français) **:** courriel, généralement commercial, envoyé massivement à des listes d'adresses constituées frauduleusement.

Spyware (**logiciel espion** en français) **:** code malveillant généralement intégré à un programme légitime pour effectuer une action de collecte d'information ; par exemple ce qui est tapé au clavier pour

récupérer des mots de passe (**keylogger** en anglais). Les informations ainsi récupérées sont ensuite automatiquement et discrètement envoyées au pirate ou celui-ci vient les chercher via une « porte dérobée » (**backdoor** en anglais).

SSI (Sécurité du Système d'Information) : « ensemble des moyens techniques, organisationnels, juridiques et humains nécessaire et mis en place pour conserver, rétablir, et garantir la sécurité du système d'information » [wikipedia]. La SSI a pour objet de contrer les menaces pesant sur le SI (environnement, pannes matérielles, erreurs humaines ou logicielles, attaques diverses…) par des mesures proportionnées aux risques.

USB (Universal Serial Bus) : norme de transmission de données (et d'énergie) entre un ordinateur et certains périphériques tels que les omniprésentes « clés USB » (mémoires amovibles)

Ver : logiciel malveillant se propageant à l'insu et sans intervention de l'utilisateur. Il tente d'infecter les ordinateurs de proche en proche via différents protocoles d'échanges entre ces machines. Par exemple par envoi automatique aux adresses contenues dans le carnet d'adresse pour un ver de type « messagerie ».

Virus : code malveillant intégré à des logiciels ou fichiers légitimes échangés par les utilisateurs (dans les pièces jointes aux messages électroniques par exemple). La nocivité d'un virus dépend du bon vouloir de son concepteur…