Charte d'utilisation
des ressources informatiques
IMT Atlantique Bretagne Pays de la Loire

Sommaire

Introduction

La présente charte (ci-après dénommée « Charte ») a pour objet de définir les conditions d'accès et les règles d'utilisation des ressources informatiques de l'IMT Atlantique Bretagne Pays de la Loire (ci-après dénommée « École ») telles que définies en annexe à cette Charte. Elle a aussi pour vocation à sensibiliser les usagers des campus aux risques liés à l'utilisation des ressources informatiques sur l'intégrité et la confidentialité des informations traitées. Ces risques imposent le respect de certaines règles de sécurité et de bonne conduite. L'imprudence ou la malveillance d'un utilisateur peuvent avoir des conséquences graves de nature à engager sa responsabilité civile et/ou pénale ainsi que celle de l'École et celle de l'IMT.

Objectifs de la charte

Le contenu

La présente Charte définit les règles d'utilisation des systèmes d'information et de communication appartenant ou concernant l'École, dans le respect des dispositions législatives, réglementaires et de sécurité. Elle précise les droits et les obligations des utilisateurs, les engagements de l'École, les moyens de contrôle utilisés par la Direction Infrastructure et Systèmes d'Information (DISI) ainsi que les mesures et/ou sanctions applicables en cas de non-respect de ces règles.

Les personnes concernées

Cette Charte s'applique à toute personne utilisant les systèmes d'information et de communication de l'École (réseaux, matériels, services, Intranet..), mis à disposition par l'École, depuis le réseau de l'École (Internet..) ou associées aux activités de l'École (ressources informatiques des partenaires par exemple).

Par Usager s'entend toute personne ayant accès, dans le cadre de l'exercice de son activité professionnelle ou académique, aux ressources du système d'information quel que soit son statut.

Ainsi sont notamment désignés :

- Tout personnel titulaire ou non titulaire, élève, vacataire, stagiaire, hébergé, invité, doctorant, post-doctorant, diplômé, etc. ;
- Tout prestataire ayant contracté avec l'École.
- Tout partenaire ayant accès aux ressources informatiques dans le cadre d'un projet

Les bases légales de la charte

Cette Charte est incluse dans le règlement intérieur de l'École, elle est associée à la charte déontologique de RENATER signée par l'École et dont les règles d'usage sont reprises dans ce

document. Ce document se fonde également sur les textes de loi et règlements mentionnés en annexe aux présentes.

Droits et obligations des usagers

Conditions d'accès aux systèmes d'information et de communication

Le droit d'accès aux systèmes d'information et de communication est personnel et incessible. Le bénéficiaire d'un compte informatique s'engage à ne pas divulguer ses identifiants. L'accès au système d'information de l'École est destiné à usage professionnel. Seuls les services présentant un lien direct avec l'activité de l'École ont vocation à être utilisés. L'utilisation à titre privé est tolérée à condition d'être raisonnable, licite et ne pas perturber le bon fonctionnement du service.

Le compte informatique

Le droit d'accès au système d'information de l'École via un compte informatique est accordé sous réserve que le bénéficiaire dudit compte ait bien lu le document réglementaire et se soit engagé à respecter les règles qui y sont stipulées. Ce document diffère selon le statut du bénéficiaire : il s'agit du règlement intérieur de l'École dans lequel cette Charte est incluse pour le personnel et les élèves, et uniquement de cette Charte pour les personnes externes (prestataires, partenaires).

La durée de vie du compte informatique est fonction du statut de l'Usager. Á titre exceptionnel des prolongations du droit d'accès peuvent être accordées sur demandes motivées, formulées par écrit.

Protection des personnes

La loi numéro 78-17 du 6 janvier 1978 modifiée en 2004 relative à l'informatique, aux fichiers et aux libertés définit les conditions dans lesquelles des traitements de données à caractère personnel peuvent être effectués. Elle accorde aux personnes concernées par les traitements, un droit d'accès et de rectification des données les concernant. L'IMT a désigné un correspondant CNIL qui s'appuie sur des correspondants informatique et liberté (CIL) locaux dans les écoles, ceux-ci ont pour rôle de veiller au respect de cette loi et de tout autre texte législatif et réglementaire, notamment le Règlement européen Général sur la Protection des Données 2016/679 du 27 avril 2016 (RGPD) qui entrera en vigueur le 25 mai 2018.

Si, dans l'accomplissement de son travail, l'Usager est amené à constituer des fichiers soumis aux dispositions de la loi informatique et liberté, il doit au préalable et en concertation avec son responsable d'entité, accomplir les formalités requises par la CNIL par l'intermédiaire du CIL local. Il doit veiller à un traitement des données conforme aux dispositions légales.

Le CIL local est donc obligatoirement consulté par le responsable des traitements (la MOA) préalablement à la mise en œuvre de l'application ou la constitution du fichier. Il référence dans un registre la liste de l'ensemble des traitements de données à caractère personnel au fur et à mesure de leur mise en œuvre. Cette liste est tenue à disposition de toute personne en faisant la demande et diffusée sur le site Intranet de l'école. Le CIL veille au respect des droits des personnes (droits d'accès aux informations, rectification et opposition).

Respect des droits de propriété des licences

L'Usager est soumis au respect des dispositions légales. En particulier il est interdit aux Usagers du système d'information de faire un usage des logiciels non conforme aux prescriptions

de son auteur ou de la société qui le met à disposition ou aux stipulations des licences les régissant, ainsi que de publier tout document protégé par les textes relatifs à la propriété littéraire et artistique.

Il est également interdit d'installer sur les équipements de l'École mis à disposition des logiciels contrefaits ou pour lesquels l'École n'aurait pas de licence.

Respect du caractère confidentiel des informations

Les Usagers ne doivent pas tenter de :

- Lire, copier, modifier les fichiers d'un autre Usager sans son autorisation ;
- Intercepter les communications privées entre Usagers, qu'elles se composent de courrier électronique ou de dialogues directs ;
- Utiliser un compte autre que celui dont il bénéficie;
- Effectuer de manœuvres qui auraient pour but de méprendre les autres Usagers sur leur identité ;
- S'approprier ou de décrypter le mot de passe des autres Usagers;
- Limiter ou d'interdire l'accès aux systèmes d'information et de communication à des Usagers autorisés ;
- Réaliser des copies de fichiers ou données de l'École sans son autorisation

Responsabilités de l'usager

Chaque Usager est responsable de l'usage qu'il fait des systèmes d'information et de communication de l'École, ainsi que de l'ensemble des informations qu'il met à la disposition du public. Il reconnait également que toute violation des dispositions de la présente Charte ainsi que, plus généralement, tout dommage causé à l'École ou à un tiers engagera sa responsabilité.

Chaque titulaire de compte informatique, ou d'un dispositif lui permettant d'accéder au réseau, est responsable des opérations locales ou distantes effectuées depuis son compte ou sous le couvert de dispositifs qui lui ont été attribués.

Toutes les données, informations, documents et fichiers et leurs reproductions (« Données »), transmis par l'École à l'Usager ou auxquels il a eu accès à l'occasion de son (ses) séjour(s) ou visites à l'École, resteront la propriété de l'École sous réserve des droits des tiers.
Ces Données devront être restituées à l'École ou détruites, par l'Usager, sur sa demande ou lors de la suppression de son compte informatique.

Administration du système d'information

Obligations de l'école

L'École fait bénéficier l'Usager d'un accès aux systèmes d'information et de communication. L'Usager dispose ainsi de nombreux services, en fonction de son profil.

La DISI assure le bon fonctionnement et la sécurité des réseaux et des moyens informatiques de l'École. Les membres de la DISI disposent d'outils techniques afin de procéder à la maintenance, aux investigations et au contrôle de l'utilisation des moyens mis en place en corrélation avec l'objet de cette Charte.

Collecte et traitement des informations

Pour des nécessités de maintenance, de gestion technique, de contrôle à des fins statistiques, de traçabilité, d'optimisation, de sécurité ou de détection des abus, l'utilisation des ressources informatiques et des services réseau peut être contrôlé et analysé dans le respect de la législation applicable et notamment au regard de la loi informatique et libertés et du RGPD.

L'École est dans l'obligation légale de mettre en place un système de journalisation des accès Internet, de la messagerie et des données échangées entre les Usagers. Seules les données d'accès et métadonnées associées à ces échanges sont journalisées.

La DISI traite les données collectées conformément aux principes de la CNIL et aux déclarations faites par l'École, mentionnant notamment la durée de conservation des traces et la durée de connexion, en application de la loi en vigueur et du RGPD.

Systèmes automatiques de filtrage

Á titre préventif et afin d'assurer la sécurité et la confidentialité des données, des systèmes automatiques de filtrage permettant de diminuer les flux d'information sont mis en œuvre. Il s'agit notamment de filtrage de sites Internet, de l'élimination ou de la mise en quarantaine de courriels non sollicités ou incorporant un virus, du blocage de certains protocoles…

Systèmes automatiques de traçabilité

La DISI opère sans avertissement les investigations nécessaires à la résolution de dysfonctionnements des systèmes d'information et de communication ou de l'un de ses composants, qui mettent en péril son fonctionnement ou son intégrité. Elle s'appuie pour ce faire, sur des fichiers de journalisation (fichiers « log ») qui recensent toutes les connexions et tentatives de connexions aux systèmes d'information. La DISI est la seule entité utilisatrice de ces informations qui sont effacées selon les délais légaux.

Gestion du parc informatique

La DISI dispose d'outil de gestion du parc informatique. Celui-ci permet la gestion de l'inventaire des composantes matérielles et logicielles des différents équipements informatiques. Un outil est systématiquement déployé sur l'ensemble des appareils connectés et gérés par l'École. Il ne doit en aucun cas être désinstallé par l'Usager.

Á des fins d'assistance, la DISI peut accéder à la session de travail de l'Usager par prise en mains à distance après l'autorisation expresse de ce dernier.

Dans le contexte de mise à jour et évolution du système d'information, le personnel de la DISI peut être amené à intervenir sur l'environnement technique des postes de travail. Il s'interdit d'accéder aux contenus de l'Usager qui ne sont pas en rapport direct avec les nécessités de son intervention technique.

Règles générales d'utilisation

Utilisation raisonnée

Les Usagers s'engagent à adopter les bonnes pratiques d'utilisation des systèmes d'information et de communication visant notamment à :

- Garantir la sécurité et l'intégrité du SI de l'École ;
- Réduire l'empreinte énergétique de l'École ;
- Rendre le système d'information et de communication le plus efficient possible ;

Utilisation du matériel informatique

Les Usagers s'engagent à respecter les règles d'accès aux salles contenant du matériel informatique, notamment :

- En réservant au préalable la salle si besoin
- En prenant soin du matériel mis à disposition

L'Usager s'engage à prendre soin de tout matériel mis à sa disposition par l'École et à signaler tout dysfonctionnement constaté via le guichet des demandes d'intervention.

Le matériel informatique de l'École ne doit être utilisé que dans le cadre des missions de l'École, y compris le matériel nomade tels que les ordinateurs portables et smartphones, quel que soit leur lieu d'utilisation. Un usage modéré à des fins personnelles est toléré.

L'apport de l'ordinateur personnel (BYOD) est toléré par la DISI qui n'en assure pas le support. L'usage de ce matériel ne doit pas altérer le fonctionnement ni la sécurité des systèmes d'information et de communication de l'École. La DISI ne pourra en aucun cas être responsable des dommages éventuels causés sur l'équipement personnel en cas d'intervention.

Données personnelles

Les courriels ne sont pas considérés comme personnels du simple fait de leur classement dans « mes documents » ou dans un dossier identifié par le nom ou les initiales de l'employé. Toutefois, un Usager a le droit, même au travail, au respect de sa vie privée et au secret de ses correspondances privées. Afin que ces informations soient protégées, les messages personnels doivent être clairement identifiés, par exemple :

- En précisant dans leur objet les mots clés « personnel » ou « privé »
- En les stockant dans un répertoire intitulé « personnel » ou « privé ».

Cette protection peut être levée dans le cadre d'une procédure pénale ou par décision de justice. En cas de litige, il appartient aux tribunaux d'apprécier la régularité et la proportionnalité de l'accès par l'école à ce type de messagerie.

Ainsi, par défaut les fichiers ont un caractère professionnel et l'École peut y accéder librement. Lorsque les fichiers sont identifiés comme personnels ou privés, l'École ne peut y accéder que :

- En présence de l'Usager ou après avoir obtenu son consentement
- En cas de risque ou événement particulier, qu'il appartient aux juridictions d'apprécier.

Mise en garde contre l'externalisation des données de l'École

La DISI met tout particulièrement en garde les Usagers contre l'externalisation des données confidentielles issues de l'administration, de la recherche, de l'innovation ou de l'enseignement de l'École. Ces données ne doivent pas être hébergées sur des systèmes d'information et de communication privés sans l'accord préalable de la direction de l'École.

Cette externalisation peut revêtir plusieurs formes (liste non exhaustive) :

- L'utilisation de services de messagerie et de communication, de stockage ou de partage de données n'appartenant ni à l'École ni à l'IMT.
- L'utilisation d'équipements nomades (ordinateur, portable, smartphoe, tablette…) de l'École ou l'enregistrement de données confidentielles sur du matériel personnel. Quand cela est techniquement possible ces équipements doivent faire l'objet d'une sécurisation particulière au regard de la sensibilité des documents qu'ils peuvent stocker, notamment par le chiffrement.

L'utilisation d'outils personnels (smartphones, tablettes..) pour relever sa messagerie électronique comporte des risques particuliers pour la confidentialité des messages, notamment en cas de perte ou de vol de ces équipements. Quand ces appareils ne sont pas utilisés durant quelques minutes, ils doivent disposer d'un mécanisme de verrouillage automatique afin de prévenir tout accès non autorisé aux données contenues.

Règles de sécurité

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

- Signaler à la DISI toute atteinte ou tentative de violation suspectée de son compte informatique et de manière générale tout dysfonctionnement ;
- Le changement de mot de passe est assujetti à un algorithme qui permet d'en vérifier la robustesse. Il n'est pas imposé de règle temporelle dans le changement du mot de passe, cependant il est impératif de modifier celui-ci en cas de soupçon sur son éventuelle violation ;
- Ne jamais divulguer son identifiant/mot de passe
- Ne jamais demander les identifiants/mot de passe à un collègue ou collaborateur ;
- Ne pas masquer son identité ;
- Ne pas usurper l'identité d'autrui ;
- Ne pas modifier le paramétrage des matériels de l'École ;
- Ne pas installer sans autorisation, ne pas copier, modifier et détruire les logiciels propriété de l'École ;
- Verrouiller son ordinateur dès qu'il quitte son poste de travail ;
- Ne pas accéder, tenter d'accéder, supprimer ou modifier des informations qui ne lui appartiennent pas.

Règles particulières d'utilisation

Réseau Intranet /Internet

Les Usagers ont accès à Internet via le réseau d'enseignement-recherche (RENATER) et aux ressources de l'École pour lesquels leur est ouvert un compte et délivré un mot de passe. Ils s'engagent à n'utiliser leur droit d'accès qu'à des fins strictement professionnelles conforment à la finalité du réseau RENATER. Une utilisation à titre privée est tolérée et doit rester raisonnable, licite et ne pas perturber le bon fonctionnement du service.

Les limites d'utilisation peuvent être éventuellement modifiées en cours d'année par la DISI. Celle-ci s'engage à diffuser ces modifications.

Pages personnelles / professionnelles

L'Usager ne doit pas stocker et mettre en consultation sur les serveurs de l'École des informations qui ne sont pas rigoureusement en rapport avec les missions de l'École. Toutefois, la création de pages personnelles à l'aide de moyens et du matériel de l'École est tolérée. Le contenu de ses pages ne doit poser aucun problème déontologique et doit respecter les obligations de l'Usager résultant de son statut et de son contrat

Personnel ayant accès à des données confidentielles

Les personnels qui, de par leur fonction, possèdent des droits plus étendus leur permettant d'avoir accès à des informations confidentielles sont tenus de respecter le secret professionnel. Ils doivent s'abstenir de toute intervention susceptible de compromettre la sécurité et le fonctionnement du Système d'Information de l'École

Les personnels en charge des opérations de contrôle sont soumis à une obligation de confidentialité. Ils ne peuvent donc pas divulguer les informations qu'ils sont amenéss à connaitre dans la cadre de leur fonction. En particulier lorsqu'elles sont couvertes par le secret des correspondances ou relèvent de la vie privée de l'Usager, dès lors que ces informations sont conformes aux lois et règlements en vigueur.

Responsabilité-Sanctions

Mesures/Sanctions applicables en cas de non-respect des règles

Le non-respect des règles établies ou rappelées par la présente Charte pourra donner lieu, indépendamment des éventuelles sanctions pénales telles que prévues par les lois et règlements en vigueur, à la mise en œuvre des mesures suivantes :

- **Sanctions disciplinaires** : Les sanctions disciplinaires concernant les personnels et les élèves sont précisées dans le règlement intérieur de l'École.
- **Suspension de l'accès aux services** : l'Usager qui enfreint l'une des règles énoncées dans la présente Charte s'expose à la suspension de son accès aux ressources informatiques notamment à l'Internet jusqu'à ce que la direction ait statué sur les éventuelles suites à donner.

La DISI peut aussi en cas d'urgence (ou à la demande d'autorités de régulation CERTA, CERT RENATER…) :

- Limiter ou interrompre temporairement l'accès d'un Usager aux applications de l'École et au réseau Internet avec ou sans préavis suivant la gravité de la situation ;
- Isoler ou neutraliser provisoirement toute donnée, serveur ou fichier manifestement non conforme aux dispositions de la présente Charte ou qui mettrait en péril la sécurité des moyens informatiques.

Suite à une telle intervention, la DISI s'engage à contacter au plus vite l'Usager concerné et le cas échéant son responsable afin de régulariser la situation.

Annexes

Charte déontologique RENATER

http://www.renater.fr/IMG/pdf/charte_fr.pdf

Dispositions légales applicables

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

Règlement européen Général sur la Protection des Données 2016/679 du 27 avril 2016 (RGPD) qui entrera en vigueur le 25 mai 2018

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

Dispositions Pénales :
Code Pénal (partie législative) : art 226-16 à 226-24
Code Pénal (partie réglementaire) : art R. 625-10 à R. 625-13
Loi n°88-19 du 5 janvier 1988 relative à la fraude informatique dite loi Godfrain.
Dispositions Pénales : art 323-1 à 323-3 du Code Pénal.
Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN)
Loi n°94-361 du 10 mai 1994 sur la propriété intellectuelle des logiciels.
Disposition Pénale : art L.335-2 du Code Pénal.

Glossaire

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.
Caractère raisonnable : Le caractère raisonnable dépend du temps passé dans l'utilisation en mode privé, du caractère licite, des risques que l'utilisation fait courir à la sécurité du SI, de l'éventuelle mise en cause de la responsabilité de l'école et de son image.
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.

Contrat de licence d'un logiciel : Contrat par lequel le titulaire des droits sur un programme informatique définit avec son cocontractant (exploitant ou utilisateur) les conditions dans lesquelles ce programme peut être utilisé, diffusé ou modifié.

DISI (Direction de l'Infrastructure et des Systèmes d'Information) : service en charge de la gestion de l'infrastructure et du système d'information de l'établissement (ensemble de services numériques mis à la disposition des communautés enseignement, recherche et administration de l'établissement). Il en assure l'exploitation au quotidien et son évolution dans le cadre du schéma directeur du système d'information.

Guichet des demandes d'intervention : Outil logiciel permettant de centraliser l'ensemble des demandes d'intervention.

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.

Logiciel libre et logiciel open-source : un **logiciel libre** est un logiciel qui peut être utilisé, modifié et redistribué sans restriction par la personne à qui il a été distribué. Un logiciel **Open Source** est un programme informatique dont le code **source** est distribué sous une licence permettant à quiconque de lire, modifier ou redistribuer ce logiciel.

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.

RENATER (Réseau National de télécommunications pour la Technologie l'Enseignement et la Recherche) : interconnecte les établissements, directement ou via des réseaux de collecte ayant une activité dans les domaines de la recherche, la technologie et l'enseignement. RENATER assure la connectivité Internet nationale et internationale.

Ressources informatiques : regroupe l'ensemble des matériels (ordinateurs, téléphones, copieurs, smartphone, tablettes…) les logiciels, les procédures informatisées, les données numériques et les fichiers informatiques.

RSSI (Responsable de la Sécurité du Système d'Information) : nommé par la direction, il a pour mission l'élaboration et la mise en mise en œuvre de la politique de sécurité du système d'information de l'établissement.

Responsable des traitements : la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens. Voir :
https://www.cnil.fr/sites/default/files/typo/document/20100201_NE_RESPONSABLE_DE_TRAITEMENT_VD.pdf

Schéma Directeur du Système d'Information : plan stratégique du développement du système d'information. 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. 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.

Système d'information et de communication : ensemble des éléments participant à la gestion, au traitement, au transport et à la diffusion de l'information au sein de l'établissement.

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...