Version 1.0 du 29 novembre 2024

Charte de l'utilisateur des systèmes d'information et de communication de l'Institut Mines-Télécom et de ses écoles

Approuvée par le Conseil d'administration de l'Institut Mines-Télécom le 29 novembre 2024

Annexe 1 du Règlement intérieur de l'Institut Mines-Télécom complétée par la charte RENATER

Institut Mines-Télécom

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

PRÉAMBULE

La présente charte, qui s'inscrit dans les objectifs de la Politique de Sécurité des Systèmes d'Information (PSSI) de l'Institut Mines-Télécom (IMT) et de ses écoles, a pour but de faire connaître les principes d'accès et d'usage au système d'information et de communication de l'IMT, ainsi que les concepts de sécurité applicables.

ARTICLE 1 : CHAMP D'APPLICATION

Les présentes dispositions concernent l'utilisation des ressources numériques de l'IMT et de ses écoles ainsi que toutes les ressources numériques extérieures auquel il est possible d'accéder depuis L'IMT et ses écoles : données, logiciels, matériels, identifiants, nom de domaines, systèmes d'information tiers internes ou non et sous réserve des dispositions prises par ces organismes.

Elles s'appliquent à toute personne physique ou morale soumise au règlement intérieur.

L'IMT et ses écoles bénéficiant entre autres d'un accès au réseau Internet via le Réseau National de Télécommunications pour la Technologie l'Enseignement et la Recherche, a adopté la charte déontologique RENATER dédiée à cet accès. Cette charte, ainsi que la liste de l'ensemble des services numériques que propose la DSI sont disponibles sur les sites web de chacune des entités de l'IMT.

Tout agissement contraire aux dispositions de la présente charte peut entraîner une suspension temporaire ou définitive des droits d'accès au système d'information et de communication, et est passible, selon la gravité des faits, de sanctions disciplinaires, civiles ou pénales.

Cette charte est annexée au règlement intérieur de l'IMT. L'acceptation du règlement intérieur entraîne de facto l'acceptation de la présente charte.

ARTICLE 2 : DÉFINITIONS

Section 2.1 École

Il s'agit d'une des écoles composant l'Institut Mines-Télécom. Elles sont au nombre de 8. Il s'agit de IMT Mines Albi, IMT Mines-Alès, IMT Atlantique, Institut Mines-Télécom Business-School, IMT Nord Europe, Mines Saint-Étienne, Télécom Paris, et Télécom SudParis.

Section 2.2 Ressources informatiques

Le terme « ressources informatiques » désigne :

- les données de l'IMT et de ses écoles ainsi que celles qui leur sont confiées ou collectées,
- les équipements informatiques et téléphoniques ;
- les moyens de stockage, archivage et sauvegarde ;
- les moyens de calcul ou de gestion ;
- les progiciels concédés à l'IMT et ses école ;
- toute ressource numérique de l'IMT et ses écoles accessible à distance, directement ou en cascade à partir des réseaux administrés par l'IMT et de ses écoles.

Section 2.3 Services numériques

Un service numérique permet à l'utilisateur de créer, de traiter ou de stocker des données sous forme numérique ou d'y accéder, ou un service numérique permet le partage ou toute autre interaction avec des données sous forme numérique qui sont téléversées ou créées par l'utilisateur ou d'autres utilisateurs de ce service.

Section 2.4 Utilisateurs

Les personnes utilisant ou ayant un accès de nature physique ou logique aux ressources informatiques et aux services numériques sont appelées « utilisateurs ». Ils sont répartis selon les catégories décrites à l'article 1.

Section 2.5 Administrateurs système d'information et de communication

Le terme d'« administrateur » recouvre les personnes expressément désignées comme tel par l'IMT ou par le prestataire de l'IMT , ayant des droits d'accès étendus aux systèmes d'information et de communication de l'IMT à des fins d'administration, maintenance ou assistance sur les données et/ou des ressources les supportant, les transportant ou les traitant, dans le cadre de son activité professionnelle et quel que soit son statut. Un administrateur peut être un membre du personnel de l'IMT ou un membre du personnel d'un prestataire de l'IMT. Tous les administrateurs appliquent la politique de sécurité des systèmes d'information et de communication de l'IMT et de ses écoles. Leurs droits et devoirs font l'objet d'une charte spécifique, figurant en annexe du règlement intérieur.

ARTICLE 3 : ACCÈS AUX RESSOURCES INFORMATIQUES ET TÉLÉPHONIQUES

Section 3.1 Autorisation d'accès au système d'information et de communication

L'accès par chaque utilisateur aux ressources informatiques et services numériques sont motivés par ses activités réalisées au sein de l'IMT ; Il se concrétise par l'ouverture d'un compte ou le droit de connecter un équipement informatique ou téléphonique sur le réseau de l'IMT et de ses écoles.

En cas d'évènement ou de risque particulier pour l'IMT, l'administrateur des ressources ou services numériques impactés peut accéder aux fichiers, dossiers et données des utilisateurs des systèmes d'information et de communication de l'IMT identifiés comme personnels en l'absence de l'utilisateur si le maintien en condition de sécurité du système d'information l'exige.

Section 3.2 Imputabilité des accès

Cette autorisation est strictement personnelle et ne peut donc en aucun cas être cédée à un tiers, même temporairement.

Les actions effectuées avec une autorisation d'accès sont imputables à l'utilisateur détenteur de cette autorisation.

Section 3.3 Utilisation des ressources

L'utilisation des systèmes d'information et de communication est limitée à des activités légitimes et légales de recherche, d'enseignement, de développements techniques, de transferts de technologies, de diffusion d'informations scientifiques, techniques et culturelles, et à toute activité administrative de gestion et de support liée à ces activités.

Ces moyens ne peuvent être utilisés pour une finalité extérieure à l'École ou plus globalement à l'IMT, sauf autorisation préalable de l'entité concernée.

Section 3.4 Annulation de l'autorisation d'accès

En raison d'une menace avérée ou d'un soupçon de menace sur son système d'information et de communication, et sur appréciation du RSSI ou de la DSI de l'entité, en cas d'absence de ce dernier, l'IMT et ses écoles se réservent le droit de retirer à tout moment cette autorisation, et ce sans préavis. Lors d'un tel événement, la DSI informera les utilisateurs impactés dans la mesure de ses moyens.

Section 3.5 Modification et cessation d'activités

Cette autorisation prend fin lors de la cessation de l'activité de l'utilisateur. Elle est réexaminée lors de toute modification d'activité (changement de service, changement de catégorie d'utilisateur). L'Institut Mines-Télécom et ses écoles peuvent accéder aux données professionnelles de l'utilisateur dans les conditions fixées par la charte de l'administrateur des systèmes d'information et de communication de l'Institut Mines-Télécom et ses écoles (voir section 2.5).

Section 3.6 Fermeture des accès, restitution des matériels en prêt

Lors de la fermeture ou de la modification de ses accès au système d'information accompagnant une mutation, un départ définitif ou une absence de longue durée (exemples : sans traitement, congé longue maladie, etc.), l'utilisateur doit laisser ses données professionnelles à disposition

de l'IMT et de ses écoles. Dans le cas contraire, l'IMT et ses écoles peuvent y accéder dans les conditions fixées par cette charte (voir section 2.5).

L'utilisateur est responsable avant son départ de la destruction de ses données privées, et l'IMT se décharge de toute utilisation frauduleuse qui pourrait en être fait si celles-ci n'ont pas été correctement supprimées.

Tous les matériels informatiques achetés sur le budget de l'IMT et ses écoles demeurent propriété de l'IMT et ses écoles. Avant son départ, que ce soit pour un départ définitif ou temporaire, un utilisateur doit restituer à son responsable hiérarchique l'ensemble de ces matériels qui lui avaient été attribués pour permettre son activité professionnelle.

Section 3.7 Boîtes de messagerie électronique de L'IMT et de ses écoles

Tout utilisateur en possession d'une boite courriels IMT ou d'un alias de redirection de messagerie justifié par un besoin professionnel, engage celui-ci à respecter l'ensemble de la présente charte pour son usage.

Section 3.8 Connexion d'équipements personnels

Toute connexion d'un équipement privé sur les systèmes d'information et de communication de l'IMT et de ses écoles engage la responsabilité de son propriétaire et se fait dans le cadre d'usages professionnels et des règles de sécurité afférentes (chartes spécifiques, réglementations particulières, etc.).

Section 3.9 Usage raisonné des ressources communes

Tout utilisateur s'engage à utiliser correctement les ressources mises à sa disposition (exemples : mémoire à ne pas saturer, espace disque, bande passante des réseaux, imprimantes, etc.). En outre, par principe de sobriété numérique, les chaînes de courriel, ou l'envoi d'une pièce jointe lourde à une liste de diffusion sont déconseillés.

Les fichiers, courriers électroniques et plus généralement toute information traitée ne sont pas considérés comme personnels du simple fait de leur classement dans un répertoire « mes documents » ou dans un dossier identifié par les initiales de l'employé. Toutefois, au titre du secret des correspondances[1], tout utilisateur a le droit, même au travail, au respect de sa vie privée et au secret de ses correspondances privées. Pour qu'ils soient protégés, ils doivent être identifiés comme tels.

Exemples :

- en précisant dans l'objet « Personnel » ou « Privé » ;

- en les stockant dans un répertoire intitulé « Personnel » ou « Privé ».

Section 3.10 Usage raisonné de la téléphonie

Le titulaire d'un téléphone mobile, d'une tablette, ou tout autre matériel de communication mobile avec un forfait téléphonique professionnel fournis par l'IMT et ses écoles s'engage à faire une utilisation raisonnée des communications. En particulier il reste vigilant lors de l'utilisation des

[1] *Articles 226-15 et 432-9 du code pénal et L33-1 du code des postes et communications électroniques.*

options data, notamment lors de ses déplacements à l'étranger.

En cas d'utilisation non professionnelle et abusive, occasionnant un dépassement du forfait mobile alloué ou des consommations hors forfait, l'IMT et ses écoles prendront les mesures adéquates pour faire cesser cet abus. L'IMT exigera le remboursement de la contre-valeur de l'utilisation non professionnelle imputée à l'utilisateur.

Afin de maîtriser les coûts, l'utilisateur doit privilégier la connexion Wifi lorsqu'elle existe, au détriment d'une connexion réseau mobile via un forfait souscrit par l'IMT et ses écoles. Dans ce cas, il est recommandé d'activer lors de la connexion au réseau Wifi le service VPN fournit par la DSI de son entité s'il en bénéficie (voir section 4.12).

ARTICLE 4 : RÈGLES GÉNÉRALES DE SÉCURITÉ

Tout utilisateur est responsable de l'utilisation qu'il fait des ressources informatiques et services numériques de l'IMT et de ses écoles. Il doit donc, à son niveau, contribuer à la sécurité, afin de ne pas constituer lui-même un élément de faiblesse pour le système d'information et de communication de l'IMT et de ses écoles. En particulier :

Section 4.1 Gestion des authentifiants informatiques

Tout utilisateur doit choisir des mots de passe sûrs respectant à minima les recommandations de la PSSI de l'IMT et de ses écoles. L'administrateur peut en tester la robustesse. L'utilisateur doit faire usage du coffre-fort des mots de passe dès lors que cette solution est proposée par son entité.

Ces mots de passe doivent être gardés secrets ; ils ne doivent pas être écrits ; ils ne doivent pas être enregistrés dans des systèmes externes à l'IMT et ses écoles (exemple : synchronisation des mots de passe via un navigateur), et en aucun cas être communiqués à des tiers.

À la demande des administrateurs, ils doivent être changés.

Section 4.2 Usurpation d'identité

Chaque compte est personnel et correspond à des privilèges en rapport avec l'activité de l'utilisateur.

Un utilisateur ne doit pas utiliser de comptes autres que ceux pour lesquels il a reçu une autorisation.

Il doit s'abstenir de toute tentative de s'approprier le mot de passe d'un autre utilisateur, sous peine de sanctions disciplinaires ou judiciaires.

Toute session associée à un compte d'un utilisateur est strictement personnelle. Les utilisateurs ne doivent pas s'éloigner d'un équipement informatique ou téléphonique mobile sans avoir préalablement verrouillé sa session.

Section 4.3 Mise en œuvre d'outils ayant un impact sur la sécurité du SI

L'utilisation ou le développement de programmes informatiques ou la mise en œuvre de technologies mettant sciemment en cause la sécurité des systèmes d'information et de communication de l'IMT et de ses écoles ou des réseaux nationaux ou internationaux (exemples : virus, codes infinis, scanners de vulnérabilités, etc.), sont interdits.

A l'exception d'un usage légitime, l'utilisateur s'expose à des sanctions disciplinaires ou des éventuelles poursuites que l'École ou l'autorité judiciaire seraient en droit d'engager[2].

Section 4.4 Devoir de rendre compte

Un utilisateur doit signaler toute violation, tentative de violation ou soupçon de violation des systèmes d'information et de communication dans les délais les plus brefs aux responsables de la sécurité de son entité (RSSI, Officier de sécurité et leurs suppléants, DSI).

Section 4.5 Raccordement des équipements informatiques

La connexion temporaire d'un ordinateur ou téléphone mobile privé aux réseaux accessibles sur les campus de l'IMT et de ses écoles est autorisée dans le respect de la PSSI de l'IMT et de toute politique de sécurité spécifique lorsque qu'elle s'applique.

[2] *Atteintes aux systèmes de traitement automatisé de données (Articles 323-1 à 323-8)*

Conformément à la charte, les administrateurs se réservent le droit de bloquer à tout instant, tout équipement ne respectant pas cette règle.

Section 4.6 Constatation de failles de sécurité

Les utilisateurs s'engagent à ne pas exploiter les éventuelles failles de sécurité, anomalies de fonctionnement, ou défauts de configuration concernant toute ressource informatique.

Ils doivent les signaler dans les meilleurs délais, et en priorité aux personnels de la DSI ou à l'administrateur de la ressource informatique, en mettant en copie le RSSI et son suppléant. Ils s'engagent à ne pas la communiquer publiquement.

Plus généralement, l'utilisateur doit être vigilant et signaler aux administrateurs toute anomalie, et se conformer à leurs consignes.

Section 4.7 Lutte antivirale

L'utilisateur a le devoir de protéger les équipements qu'il raccorde au système d'information et de communication de l'IMT et de ses écoles, ou de s'assurer que ceux-ci le sont (exemples : anti-virus dont les signatures virales sont à jour, mises à jour de sécurité, etc.).

Section 4.8 Sécurité des données professionnelles

Les utilisateurs doivent veiller à la sécurité de leurs données professionnelles, y compris leur courrier électronique, en termes de confidentialité, intégrité et disponibilité. Cela implique de s'assurer qu'une sauvegarde est effectuée à une fréquence adaptée au besoin métier et que leur lieu de stockage est pérenne et sécurisé.

Sauf contrainte particulière (matériel incompatible, législation propre à un pays), le chiffrement[3] est obligatoire dans le cas d'usage d'informatique nomade (ordinateurs portables, téléphone mobiles, clefs USB, disques externes, et tout support de stockage amovible de manière générale).

Dans le cas où la législation d'un pays interdirait le chiffrement ou imposerai la remise du poste de travail à une autorité locale, il est recommandé d'utiliser un poste de travail dédié et ne contenant aucune donnée pouvant avoir un impact négatif pour l'IMT et ses écoles.

L'utilisateur prend les dispositions nécessaires pour qu'une éventuelle perte de données présentes localement sur ses équipements informatiques ne pénalise pas l'Institut Mines-Télécom et ses écoles ainsi que leurs partenaires.

Pour se faire, il s'engage à enregistrer les données qu'il produit uniquement dans les espaces de stockage que l'Institut Mines-Télécom et ses écoles et les laboratoires mettent à sa disposition : serveur de fichiers, etc.

Section 4.9 Utilisation des ressources numériques de l'École en externe

L'usage de services externes (exemples : espace disques, messagerie, bureautique) et les serveurs de données (exemples : web, FTP, RDP) ne présentant pas de garantie contractuelle de confidentialité, intégrité ou disponibilité est déconseillé. Avant de faire usage de tels services, l'utilisateur doit s'assurer de l'absence de données que leur sensibilité ne rend pas éligibles à ces services (ex : données personnelles, secret industriel etc.). Dans tous les cas, il doit demander un avis auprès du personnel de la DSI ou du RSSI de son entité.

[3] *Action de rendre des données illisibles de manière réversible, à l'aide d'un mot de passe ou d'une clef numérique.*

Section 4.10 Vol d'équipements informatiques ou téléphoniques

Les utilisateurs doivent déclarer au plus vite, à leur centre d'assistance Informatique, ainsi qu'à leur supérieur hiérarchique dont ils dépendent tout vol de matériel informatique ou téléphonique. Ces services prennent ensuite les mesures appropriées.

Un dépôt de plainte doit être fait par l'utilisateur qui communiquera la copie du récépissé à la DSI dont il dépend.

Section 4.11 Connexion aux réseaux sans fil

Les utilisateurs doivent être vigilants lors de connexions à des réseaux sans fil peu sécurisés, notamment dans les lieux publics. La sécurité de ces réseaux est faible quand ce ne sont pas des leurres destinés à intercepter les identifiants de l'utilisateur. Dans ce cadre, l'utilisation d'outil de type VPN, est recommandée.

Section 4.12 Réglementation des autorités de tutelle

Lorsqu'ils sont concernés, les utilisateurs doivent respecter les règles définies par leurs autorités de tutelle (exemple : CNRS), tant que celles-ci sont compatibles avec les règles de l'Institut Mines-Télécom et ses écoles. En cas d'incompatibilités, l'utilisateur doit se rapprocher de la DSI de son entité de rattachement, afin de connaître la conduite à tenir.

Les règles de sécurité de l'IMT prévalent toujours dans les locaux de l'IMT et ses écoles.

Section 4.13 Intégrité des services numériques et applications imposés par toute Direction des systèmes d'information de l'IMT

Il est interdit de procéder à la modification l'altération, la désinstallation ou le blocage du bon fonctionnement de toute application ou service que la DSI installe sur les équipements informatiques et téléphoniques dont elle a la responsabilité. La liste de ces services et applications est disponible sur demande auprès de la DSI.

ARTICLE 5 : RESPECT DE LA PROPRIÉTÉ INTELLECTUELLE

Section 5.1 Reproduction ou décompilation de logiciels

La reproduction des logiciels commerciaux autre que pour l'établissement d'une copie de sauvegarde par le détenteur légal du droit d'usage concédé est interdite. La décompilation de logiciels propriétaires est strictement encadrée par la loi[4].

Section 5.2 Installation de contenus numériques soumis aux copyrights, droits d'auteur ou DRM

Il est interdit d'installer sur le système d'information et de communication de l'IMT et de ses écoles ou sur tout matériel connecté à ce SI un logiciel, une police de caractères ou tout autre fichier en violation des droits d'auteur, copyrights, gestion des droits numériques (DRM) et licences associées.

Les conditions d'utilisation des licences des logiciels libres doivent naturellement être respectées.

Section 5.3 Logiciels professionnels installés sur un équipement privé

Les logiciels professionnels mis à disposition par l'IMT et ses écoles sur des équipements informatiques ou téléphoniques personnels doivent être supprimés lors du départ de l'utilisateur de l'IMT ou de l'école concernée ou d'un de ses laboratoires, ou si leur usage n'est plus justifié.

Section 5.4 Archivage des ressources documentaires

En dehors des sauvegardes prévues dans le cadre de la continuité des activités (voir section 4.8), l'archivage massif et systématique de ressources documentaires internes à l'IMT, ses écoles et ses laboratoires (exemple : sites web, fichiers, etc.) par l'intermédiaire d'un robot de sauvegarde, ou de tout autre logiciel proposant la même fonctionnalité, est interdit.

[4] *Code de la propriété intellectuelle, article L122-6 et suivants.*

ARTICLE 6 : RESPECT DE LA CONFIDENTIALITÉ DES INFORMATIONS

Section 6.1 Droits d'accès aux informations

Tout utilisateur est responsable, pour ses fichiers et répertoires, des droits de lecture et de modification qu'il donne aux autres utilisateurs.

En conséquence, les utilisateurs ne doivent pas tenter de lire, copier, divulguer, modifier les fichiers d'un autre utilisateur sans y avoir été explicitement autorisés.

Section 6.2 Hébergement des informations

Les utilisateurs doivent exploiter les serveurs de partage de fichiers ou de gestion documentaire de l'IMT, ses écoles et ses laboratoires, ainsi que ceux de l'opérateur RENATER ou d'un hébergeur validé par le RSSI, le DPD (ou DPO) et la DSI dont dépend l'utilisateur (exemples : cloud CNRS, opérateur privé basé en France, niveau de certification HDS, etc.). Sauf autorisation préalable de la DSI, l'usage d'hébergements distants non maîtrisés (exemples : non-respect de la protection des données personnelles, absence de contrat de service avec l'École, soumission à toute loi pouvant porter atteinte à la souveraineté des informations est proscrit.

Section 6.3 Interception des communications entre tiers

Les utilisateurs ne doivent pas tenter d'intercepter des communications entre tiers.

Section 6.4 Respect des engagements de confidentialité avec un tiers

À leur niveau, les utilisateurs sont tenus de prendre les mesures de protection des données garantissant le respect des engagements de confidentialité pris par l'IMT et ses écoles vis à vis de tiers. En cas de doute, ils sont invités à se rapprocher de leur service de support informatique, ou à défaut du service compétent de leur établissement.

Section 6.5 Traitement des données à caractère personnel

L'Institut Mines-Télécom et l'ensemble de ses écoles sont soucieux de la protection de la vie privée des personnes physiques dont ils traitent les données personnelles, et ce, dans le respect du Règlement (UE) 2016/679 (Règlement Général sur la Protection des Données entré en application le 25 mai 2018) et de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. L'Institut Mines-Télécom et ses écoles possèdent une politique générale de protection des données à caractère personnel. Cette politique est à destination des salariés et des agents publics de l'IMT et de l'ensemble des personnes extérieures à l'IMT.

Tout traitement de données à caractère personnel mis en œuvre pour le compte de l'IMT doit être déclaré au délégué à la protection des données compétent de l'IMT et respecter le cadre légal applicable. Le délégué à la protection des données (DPD), doit être informé de tout projet de traitement de données à caractère personnel sur le système d'information et de communication de l'Institut Mines-Télécom et ses écoles, afin d'accompagner le responsable du traitement dans la mise en conformité avec le règlement RGPD, notamment par le remplissage du registre des traitements de données à caractère personnel.

Section 6.6 Continuité de service

En cas d'absence d'un utilisateur, toute mesure indispensable à la continuité du service peut être

mise en œuvre dès lors qu'elle ne contredit pas les règles décrites dans la présente charte et dans la PSSI de l'IMT et ses écoles[5] (exemples : transfert de dossiers, droits d'accès temporaires ou permanents à des personnes ayant le besoin d'en connaître, et comportant les éventuelles habilitations requises).

Section 6.7 Confidentialité des données qualifiées de sensibles

Les utilisateurs doivent être extrêmement vigilants vis-à-vis des données considérées comme sensibles[6] que ce soit au sens réglementaire (exemple : RGPD), ainsi que dans le cas où son propriétaire l'aurait qualifiée de sensible (exemple : diffusion limitée à un cercle restreint d'utilisateurs).

En particulier, ils ne doivent pas transporter ou déposer sans protection (telle qu'un chiffrement) des données sensibles sur des supports ou services non fiabilisés.

L'accès à des données sensibles est interdit depuis des postes ou des réseaux non sûrs.

Les utilisateurs doivent préférentiellement partager leurs données via un serveur de fichiers ou un serveur de gestion documentaire autorisés par la DSI, ou le RSSI (ou son suppléant) de l'entité dont il dépend, à défaut un service de messagerie de l'IMT et ses écoles.

Afin de préserver la confidentialité des informations traitées par les messageries électroniques de l'IMT, les redirections automatiques vers une messagerie externe à l'IMT sont interdites.

Lors de consultations d'informations sensibles, les utilisateurs doivent être vigilants quant aux traces laissées : (exemples : historique de navigateurs, mots de passe, caches, cookies, etc.).

[5] La messagerie électronique institutionnelle fait exception (clôture puis destruction du compte de messagerie au-delà de la durée minimale définie à la section 3.7).

[6] Une donnée est considérée comme sensible si sa divulgation, sa modification frauduleuse ou sa destruction peut porter atteinte au bon fonctionnement d'un organisme. Certaines données à caractère personnel sont considérées comme sensibles au sens du RGPD.

ARTICLE 7 : RELATIONS AVEC LES SITES DISTANTS

Section 7.1 Connexion à un site distant

Il est interdit de se connecter ou d'essayer de s'authentifier à un site distant sans que celui-ci ait dûment fourni une autorisation impliquant une authentification légitime réussie.

Tout VPN ou chiffrement réseau mis en œuvre dans un but illégitime ou a fortiori illégal est interdit.

Section 7.2 Fonctionnement intègre des systèmes d'information et de communication

Il est interdit de se livrer :

- depuis des ressources informatiques appartenant à l'IMT et ses écoles,
- ou en étant connecté aux réseaux informatiques de l'IMT et ses écoles,

à des actes mettant sciemment en péril la sécurité ou le fonctionnement des systèmes d'information locaux ou distants, et des réseaux de télécommunications ou nuire à la réputation de l'IMT et ses Écoles (exemple : redirection des noms de domaine institutionnels vers un site web non maîtrisé).

Section 7.3 Partage d'informations avec un site distant

Les utilisateurs doivent être vigilants lors de toute saisie d'informations personnelles sur Internet, notamment avec la multiplication des courriels d'hameçonnage (phishing).

L'IMT et ses écoles ne pourront être tenus responsables des dommages subis lors de telles divulgations d'informations.

Dans le respect de la législation en vigueur, l'administrateur ou la DSI se réservent le droit de bloquer les accès d'un utilisateur victime d'une attaque cyber (exemple : hameçonnage réussi d'une boite courriels) à des fins de protection des systèmes d'information et de communication et d'audit, et ce pour toute la durée qu'ils estiment nécessaire.

Dans un objectif de sensibilisation à la sécurité des informations, le RSSI ou son suppléant peuvent organiser des simulations d'attaque (exemples : hameçonnage, crise cyber) sur tout ou partie des utilisateurs. Les résultats de cette simulation sont confidentiels, et ne peuvent être exploités dans un but de notation ou mesure d'une performance d'un utilisateur.

ARTICLE 8 : ÉCHANGES ÉLECTRONIQUES

Section 8.1 Devoir de réserve

Dans ses échanges, nul ne peut :

- s'exprimer au nom de l'IMT et ses écoles,
- ou engager l'IMT et ses écoles sans y avoir été dûment autorisé,

sans que les fonctions qu'il exerce le prévoient.

Section 8.2 Règles de savoir-vivre

Chacun doit faire preuve de la plus grande correction à l'égard de ses interlocuteurs dans les échanges électroniques (courriels, chats, réseaux sociaux, blogues, etc.). Tout commentaire ou propos dégradant ou insultant (raciste, antisémite, islamophobe, sexiste, homophobe, transphobe, etc.) présents dans tout contenu électronique sont réprimés par la loi, et ne seront pas tolérés par l'IMT et ses écoles[7].

Section 8.3 Responsabilité de l'utilisateur relative au contenu des échanges

Compte tenu de la valeur juridique des courriels, chacun doit être vigilant sur leur contenu et s'assurer de leur conservation (un an minimum conseillé).

Section 8.4 Intégrité des échanges électroniques

Il est rappelé qu'aucune garantie de bonne transmission et de délai d'acheminement ne peut être apportée aux courriels qui sont émis ou réexpédiés hors de l'IMT et ses écoles, du fait même du fonctionnement d'Internet.

Section 8.5 Publications sur un site Internet hébergé par l'IMT et ses écoles

Il est rappelé que toute publication sur un site Internet hébergé par l'IMT et ses écoles engage celle-ci, ainsi que son image.

ARTICLE 9 : ÉVOLUTION DE LA CHARTE

Cette charte est consultable sur les serveurs Internet de l'IMT et ses écoles, dont les Intranets. Elle est susceptible de modifications en fonction des évolutions techniques et réglementaires, des usages et de l'organisation de l'IMT et ses écoles. Seule la dernière version française fait foi, les versions en langue étrangère n'ont qu'une valeur informative.

ARTICLE 10 : SANCTIONS APPLICABLES

Tout utilisateur n'ayant pas respecté les dispositions de la présente charte est susceptible de voir suspendre ses droits d'accès et est passible de sanctions ou poursuites en rapport avec les manquements constatés.

[7] *Loi n° 2008-496 du 27 mai 2008 portant diverses dispositions d'adaptation au droit communautaire dans le domaine de la lutte contre les discriminations.*

GLOSSAIRE

[ANSSI] : Agence Nationale de la Sécurité des Systèmes d'Information. Ce service à compétence nationale est rattaché au Secrétaire général de la défense et de la sécurité nationale (SGDSN), autorité chargée d'assister le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale.

[CNIL] : Commission nationale de l'informatique et des libertés. Désigne l'autorité administrative indépendante française chargée de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'Homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

[CNRS] : Centre national de la recherche scientifique.

[DPD] : Délégué à la Protection des Données, chargé de la protection des données personnelles au sein d'une organisation.

[DRM] : Digital Rights Management, terme anglais pour Gestion des droits numériques, la protection technique des droits d'auteur et de reproduction dans le domaine numérique.

[Droits d'auteur] : Ensemble des droits dont dispose un auteur ou ses ayants droit (héritiers, sociétés de production) sur des œuvres de l'esprit originales et des droits corrélatifs du public à l'utilisation et à la réutilisation de ces œuvres sous certaines conditions.

[DSI] : Direction des systèmes d'information.

[HDS] : Hébergeur de données de santé.

[PSSI] : Politique de Sécurité des Systèmes d'Information.

[RGPD] : Règlement général sur la protection des données. Constitue le nouveau texte de référence européen en matière de protection des données à caractère personnel. Il renforce et unifie la protection des données pour les individus au sein de l'Union européenne.

[RDP] : Remote Desktop Protocol est un protocole qui permet à un utilisateur de se connecter sur un ordinateur distant Windows, afin d'accéder à des applications et des données sur ce même ordinateur distant.

[RSSI] : Responsable de la sécurité des systèmes d'information et de communication.

[Session] : En informatique et en télécommunication, une session est une période délimitée pendant laquelle un appareil informatique est en communication et réalise des opérations au service d'un client - un usager, un logiciel ou un autre appareil.

[VPN] : Virtual Private Network. Désigne une connexion inter-réseau permettant de relier deux réseaux locaux différents par un protocole de tunnel, généralement chiffré, afin de protéger le contenu des échanges contre l'espionnage ou la modification frauduleuse des données échangées.