Charte de l'utilisateur du système d'information et de communication

approuvée par le Conseil d'hygiène, de sécurité et des conditions de travail
le 23 juin 2017
approuvée par le Conseil technique d'établissement
le 05 juillet 2017

ARTICLE 1 : PRÉAMBULE

La présente charte, rédigée dans le cadre de la Politique de Sécurité des Systèmes d'Information (PSSI) de l'École polytechnique, a pour objectif de faire connaitre les principes d'accès au système d'information et de communication de l'Ecole polytechnique et les concepts de sécurité des systèmes d'information applicables.

ARTICLE 2 : CHAMP D'APPLICATION

Les présentes dispositions concernent l'utilisation des ressources numériques de l'École polytechnique ainsi que toutes les ressources numériques extérieures auquel il est possible d'accéder depuis l'École polytechnique : 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 :

- au personnel rémunéré par l'École polytechnique (y compris les stagiaires rémunérés ou non) ;
- au personnel non rémunéré par l'École polytechnique, travaillant ou accueillis dans ses locaux ;
- aux étudiants (élèves du cycle ingénieur polytechnicien, Bachelors, Graduates Degrees, Master, doctorants, autres apprenants) ;
- et d'une manière générale, à toute personne physique ou morale présente, à quelque titre que ce soit, sur le site de l'École polytechnique (visiteurs, candidats au concours, intervenants, auditeurs libres, personnels d'organismes extérieurs, prestataires, invités, collaborateurs bénévoles, membres des associations, etc.).

Le cadre légal prévaut dans l'application des règles de la présente charte. En cas de contradiction entre plusieurs textes réglementaires (exemples : politique de sécurité, code pénal, règlementation des télécommunications), seul le cadre de plus haut niveau s'applique.

L'École polytechnique bénéficiant entre autre 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[1] dédiée à cet accès. Cette charte, ainsi que la liste de l'ensemble des services numériques que propose la DSI sont disponibles sur le site web de la DSI.

La convention d'accès aux ressources du Drahi X novation Center complète la présente charte, lorsque cela est pertinent.

Tout agissement contraire aux dispositions de la présente charte peut entrainer 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'Ecole polytechnique. L'acceptation du règlement intérieur entraine de facto l'acceptation de la présente charte.

ARTICLE 3 : DEFINITIONS

Section 3.1 Ressources informatiques

Le terme « ressources informatiques » désigne les données de l'École polytechnique ou confiées à l'École ou enfin collectées par l'École, les équipements informatiques et téléphoniques, les moyens de stockage, archivage et sauvegarde, les moyens de calcul ou de gestion, les droits d'usage de progiciels concédés à l'École, ainsi que ceux auxquels il est possible d'accéder à distance, directement ou en cascade à partir des réseaux administrés par l'École polytechnique.

Tout équipement tiers éventuellement privé utilisé pour accéder à des ressources informatiques de l'École devient lui-même le temps de cet usage et pour l'application des règles énoncées dans cette charte, une ressource informatique de l'École.

Section 3.2 Services numériques

Les « services numériques » correspondent à la mise à disposition de moyens de capture, d'échange, de transformation et / ou de publication d'informations par des ressources informatiques interne ou non.

Section 3.3 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 2.

Section 3.4 Administrateurs système d'information et de communication

Le terme « administrateur système d'information et de communication » désigne tout utilisateur chargé explicitement[1] du bon fonctionnement et de la sécurité de ressources informatiques[2] faisant partie du système d'information et de communication.

Les administrateurs système d'information et de communication se divisent en deux groupes tel que décrit ci-dessous. Tous les administrateurs appliquent la politique de sécurité du système d'information et de communication de l'École polytechnique

Section 3.5 Administrateurs applicatifs

Sont administrateurs applicatifs, les utilisateurs SI en charge des activités de suivi d'exploitation (gestion des traitements et des données) liées à une application ou à un ensemble d'applications.

Ces administrateurs applicatifs sont présents dans l'ensemble des métiers de l'École (administration, enseignement, formation continue, entreprenariat, ainsi que dans les laboratoires de recherche).

Les administrateurs applicatifs sont responsables de la sécurité et du bon fonctionnement des applications placées sous leur responsabilité.

Une partie des administrateurs applicatifs sont « référents applicatifs » : Un référent applicatif est responsable de la définition des paramétrages métier et de celles des privilèges et des profils utilisateurs.

Section 3.6 Administrateurs systèmes et réseaux

Les administrateurs systèmes et réseaux ont pour mission d'installer et de gérer techniquement les ressources informatiques de l'École polytechnique. Ces administrateurs systèmes et réseaux sont principalement à la DSI et parfois dans une direction métier : dans les laboratoires de l'École polytechnique et à la direction du concours.

Les administrateurs systèmes et réseaux sont responsables techniquement de la sécurité et du bon fonctionnement des infrastructures informatiques et téléphoniques placées sous leur responsabilité.

[1] Lettre de mission, profil de poste, contrat de travail, contrat de prestation de service, etc.

[2] Équipements réseau, serveurs, systèmes d'exploitation, applications, etc.

ARTICLE 4 : ACCES AUX RESSOURCES INFORMATIQUES ET TELEPHONIQUES

Section 4.1 Autorisation d'accès au système d'information et de communication

L'utilisation des ressources informatiques est toujours motivée par un besoin métier ; elle se concrétise par l'ouverture d'un compte ou le droit de connecter un équipement informatique ou téléphonique sur le réseau de l'École polytechnique.

Section 4.2 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 4.3 Utilisation des ressources

L'utilisation du système 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, sauf autorisation préalable, formalisée par l'École polytechnique.

Section 4.4 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, l'École polytechnique se réserve 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 4.5 Modification et cessation d'activités

Cette autorisation prend fin lors de la cessation de l'activité de l'utilisateur et elle est réexaminée lors de toute modification d'activité (changement de service, changement de catégorie d'utilisateur).

Dans le cas particulier des étudiants (élèves du cycle ingénieur polytechnicien, étudiants des autres formations de l'établissement, doctorants), elle prend fin dans le délai d'un an maximum après la diplomation sauf raison exceptionnelle validée par l'École polytechnique.

Section 4.6 Fermeture des accès, restitution des matériels en prêt

Lors de la fermeture ou de la modification de ses accès accompagnant une mutation ou un départ (exemples : compte LDAP, serveur de fichiers, application, etc.), l'utilisateur doit laisser ses données professionnelles à disposition de l'École polytechnique et de son ancien service.

L'utilisateur est responsable avant son départ de la destruction de ses données privées. Avant son départ et même en cas de mutation un utilisateur doit restituer à son responsable hiérarchique l'ensemble des équipements qui lui avaient été attribués pour permettre son activité professionnelle.

Section 4.7 Responsabilité de l'utilisateur vis-à-vis des équipements

En cas de dysfonctionnement, panne ou perte d'un équipement informatique ou téléphonique ayant pour origine la négligence de l'utilisateur un remboursement à hauteur de la valeur d'usage de l'équipement pourra être exigé.

Section 4.8 Boîtes de messagerie électronique de l'École polytechnique

Sauf demande explicite de l'utilisateur auprès de la DSI, et uniquement dans un but de redirection vers une boite de messagerie électronique externe, l'adresse courriels électronique de l'École polytechnique est supprimée lors de son départ de l'École polytechnique.

Cette suppression est repoussée à cinq ans après départ de l'École polytechnique dans le cas des étudiants (élèves du cycle ingénieur polytechnicien, étudiants des autres formations de l'établissement, doctorants). Après son départ, un étudiant est libre de demander par anticipation la suppression de son adresse à tout moment.

La possession de cette adresse courriel après le départ de l'utilisateur engage celui-ci à respecter l'ensemble de la présente charte, pour l'usage de cette adresse.

Section 4.9 Connexion d'équipements personnels sur le système d'information et de communication

Toute connexion d'un équipement personnel sur le système d'information et de communication de l'École polytechnique est soumise à autorisation de la DSI, et se fait dans le cadre d'usages professionnels et des règles de sécurité de l'École polytechnique et de ses laboratoires.

L'École polytechnique ne peut être tenue pour responsable en cas de vol ou de dégradation des équipements personnels des utilisateurs.

Section 4.10 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…). Par exemple, les chaînes de courrier électronique, ou l'envoi d'une pièce jointe lourde à une liste de diffusion sont interdits.

Section 4.11 Usage raisonné de l'Internet

Seuls les services Internet présentant un lien direct et nécessaire avec l'activité professionnelle, tels que définis à la Section 4.3, ont vocation à être consultés.

Une consultation d'Internet pour un motif privé est tolérée (exemple : courriels personnels, recherches hors contexte professionnel, etc.) si elle s'inscrit dans le cadre de la Section 4.10, si elle est ponctuelle et brève, si le contenu consulté n'est pas contraire à l'ordre public et aux bonnes mœurs et enfin si cette consultation n'interfère pas outre mesure avec les missions confiées à l'utilisateur.

ARTICLE 5 : RESPONSABILITES DES ADMINISTRATEURS DU SYSTEME D'INFORMATION

Section 5.1 Attribution de droits étendus

Seuls les administrateurs jouissent de droits étendus liés à la fonction exercée et non à la position hiérarchique ou à la fiche de poste.

Section 5.2 Devoir de réserve des administrateurs

L'administrateur est soumis dans l'exercice de sa fonction à un devoir de réserve.

Pour assurer le bon fonctionnement et la sécurité du système d'information et de communication, il peut procéder aux investigations nécessaires (recherche de traces informatiques, vérification des accès, audit technique d'un poste de travail, etc.).

Pour répondre à une réquisition judiciaire, la hiérarchie pourra demander aux administrateurs de communiquer les informations obtenues dans l'exercice de leurs fonctions et entrant dans l'objet de la réquisition.

Section 5.3 Vie privée des utilisateurs

A l'exception des fichiers, répertoires, mails courriels et de façon générale toutes données qu'un utilisateur indique comme privée (exemples : l'objet d'un mail courriel est « PRIVATE », un répertoire est intitulé « Usage privé », etc.), l'administrateur peut explorer les fichiers des utilisateurs.

Lorsqu'une telle recherche est rendue nécessaire par le constat d'actes de piratage, il doit informer immédiatement le RSSI ou son suppléant, et le cas échéant le CSSI de son entité.

L'accès aux données personnelles ne peut se faire qu'en présence de l'utilisateur directement concerné, et uniquement avec son consentement écrit. Seule fait exception à cette règle le cas d'une réquisition de l'autorité judiciaire. Dans ce cas, l'administrateur systèmes et réseaux est autorisé à accéder aux données personnelles d'un utilisateur concerné par cette enquête, sans le consentement écrit de celui-ci.

Section 5.4 Gestion des traces dans le système d'information et de communication

L'administrateur assure l'enregistrement et la gestion des traces et journaux d'événements du système d'information et de communication. Il duplique et assure pendant la durée légale de conservation prévue, la sauvegarde et la conservation des traces et des journaux d'événements, prévues par la déclaration d'avis auprès de la CNIL.

Section 5.5 Gestion des sauvegardes des données des utilisateurs

Il peut réaliser la sauvegarde et l'archivage de certains disques, y compris ceux hébergeant les données des utilisateurs et le courrier électronique, afin d'assurer la continuité d'activité du système d'information et de communication.

Section 5.6 Gestion des accès d'un équipement informatiques ou téléphoniques

Il peut interdire tout flux informatique (Web, courriel, transfert de fichiers, téléphonie, vidéo, etc.), ainsi que tout équipement informatique ou téléphonique présentant des risques pour la sécurité (exemples : virus, rançongiciel, cheval de Troie, etc.), ou en infraction avec la charte ou la PSSI de l'École polytechnique.

Il peut procéder à toute recherche préventive de faille sur les équipements informatiques ou téléphoniques, privés ou non, raccordés au système d'information et de communication.

Section 5.7 Droits de configuration des équipements

En cas d'infection virale d'un équipement informatique ou téléphonique, l'administrateur pourra reconfigurer ce matériel dans un état « sortie usine », au détriment des données présentes localement.

L'utilisateur reconnait le droit à l'administrateur de réaliser cette tâche, même si elle se fait au détriment des données présentes localement sur son matériel.

Section 5.8 Devoir de l'utilisateur de sauvegarder ses données professionnelles

L'utilisateur s'engage à ce qu'une éventuelle perte de données présentes localement sur ses équipements informatiques ne pénalise pas l'École polytechnique ou ses partenaires.

Pour se faire, il s'engage à enregistrer les données qu'il produit uniquement dans les espaces de stockage que l'École polytechnique et les laboratoires mettent à sa disposition : GEIDE, serveur de fichiers, etc.

ARTICLE 6 : REGLES GENERALES DE SECURITE

Tout utilisateur est responsable de l'utilisation qu'il fait des ressources informatiques de l'École polytechnique. 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'École polytechnique. En particulier :

Section 6.1 Gestion des authentifiants informatiques

Tout utilisateur doit choisir des mots de passe sûrs respectant *à minima* les recommandations de la PSSI de l'École polytechnique. L'administrateur peut en tester la robustesse.

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'École polytechnique (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 6.2 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 ou de déchiffrer 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 s'être préalablement déconnectés de leur session.

Section 6.3 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 du système d'information et de communication de l'École polytechnique ou des réseaux nationaux ou internationaux (exemples : virus, codes infinis, scanners de vulnérabilités, etc.), sont interdits.

En particulier, l'utilisateur ne peut arguer d'une intention pédagogique ou démonstrative pour être exonéré des sanctions disciplinaires ou des éventuelles poursuites que l'École ou l'autorité judiciaire seraient en droit d'engager.

Section 6.4 Devoir de rendre compte

Un utilisateur doit signaler toute violation, tentative de violation ou soupçon de violation du système d'information et de communication dans les délais les plus brefs aux responsables de la sécurité de l'École polytechnique (RSSI, Officier de sécurité et leurs suppléants).

Section 6.5 Raccordement des équipements informatiques

L'utilisateur ne doit pas ajouter d'équipements informatiques ou téléphoniques sans autorisation d'un administrateur ou du responsable de la sécurité du système d'information et de communication.

La connexion temporaire d'un ordinateur ou téléphone mobile privé aux réseaux accessibles sur le campus de l'École polytechnique est autorisée dans le respect des règles afférentes à ces réseaux.

Conformément à la section 5.6, les administrateurs se réservent le droit de bloquer à tout instant, tout équipement ne respectant pas cette règle.

Section 6.6 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.

Ils doivent les signaler sans délais, et exclusivement à leur administrateur en mettant en copie le RSSI, et ne pas la communiquer publiquement.

L'administrateur peut toutefois prendre la responsabilité de ne pas apporter de correction, si la correction n'est pas disponible ou est considérée comme induisant d'autres problèmes, après avoir informés le RSSI et le DSI.

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

Section 6.7 Lutte antivirale

L'utilisateur a le devoir de protéger les équipements qu'il raccorde au système d'information et de communication de l'École polytechnique, 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.).

A la demande de la DSI l'utilisateur doit pouvoir prouver qu'il se conforme à cette obligation.

Section 6.8 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.

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).

Section 6.9 Utilisation des ressources numériques de l'École en externe

En cas de déplacement dans un pays dont la législation interdit le chiffrement de données, ou oblige les utilisateurs à remettre leurs mots de passe ou clefs de chiffrement aux autorités locales, les utilisateurs doivent se conformer aux lois, ne pas importer de matériels chiffrés, et ne pas transporter de données sensibles.

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.).

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

Lors de départ en mission, notamment à l'étranger, les utilisateurs doivent prendre connaissance des conseils aux voyageurs édictés par l'ANSSI (utiliser des matériels dédiés, sans données sensibles, sans données contraires aux législations locales).

Section 6.10 Vol d'équipements informatiques ou téléphoniques

Les utilisateurs doivent déclarer au plus vite à leur administrateur, ainsi qu'à leur supérieur hiérarchique et au centre d'assistance de la DSI 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.

Section 6.11 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 6.12 Règlementation des autorités de tutelle

Lorsqu'ils sont concernés, les utilisateurs doivent respecter les règles définies par leurs autorités de tutelle (exemples : CNRS, INRIA, etc.), tant que celles-ci sont compatibles avec les règles de l'École polytechnique.

ARTICLE 7 : RESPECT DE LA PROPRIETE INTELLECTUELLE

Section 7.1 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 interdite.

Section 7.2 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'École polytechnique ou tout matériel connecté à ce SI un logiciel, une police de caractères ou tout autre fichier en violation des droits d'auteur, copyrights, DRM et licences associés.

Les licences des logiciels libres doivent naturellement être respectées.

Section 7.3 Logiciels professionnels installés sur un équipement privé

Les logiciels professionnels mis à disposition par l'École polytechnique sur des équipements informatiques ou téléphoniques personnels doivent être supprimés lors du départ de l'École polytechnique ou d'un de ses laboratoires.

Section 7.4 Archivage des ressources documentaires

En dehors des sauvegardes prévues dans le cadre de la continuité des activités, l'archivage massif et systématique de ressources documentaires internes à l'École polytechnique 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.

ARTICLE 8 : RESPECT DE LA CONFIDENTIALITE DES INFORMATIONS

Section 8.1 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.

Il est cependant interdit de prendre connaissance d'informations détenues par d'autres utilisateurs, quand bien même ceux-ci ne les auraient pas correctement protégées.

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.

Le partage de fichiers depuis un poste de travail est interdit.

Section 8.2 Hébergement des informations

Les utilisateurs doivent exploiter les serveurs de partage de fichiers ou de gestion documentaire de l'École polytechnique et de ses laboratoires, ainsi que ceux de l'opérateur Renater ou d'un hébergeur validé par le RSSI ou son suppléant (exemples : cloud CNRS, opérateur privé basé en France, etc.). L'usage d'hébergements distants non maitrisés (exemples : non-respect de la protection des données personnelles, absence de contrat de service avec l'École, soumission au « patriot act » de données à usage restreint) est déconseillé (voir section 6.9).

Section 8.3 Interception des communications entre tiers

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

Section 8.4 Respect des engagements de confidentialité avec un tiers

Les utilisateurs sont tenus de prendre les mesures de protection des données garantissant le respect des engagements de confidentialité pris par l'École polytechnique vis à vis de tiers.

Section 8.5 Traitement des données nominatives

Tout traitement de données nominatives doit respecter la déclaration du traitement faite à la CNIL et le consentement recueilli lors de la collecte de ses informations. Le correspondant informatique et libertés (CIL) et à partir de mai 2018 le délégué à la protection des données (DPO), doivent être informés de tout projet de traitement de données nominatives sur le système d'information et de communication de l'École polytechnique, afin d'accompagner le responsable du traitement dans la mise en conformité avec le règlement GDPR.

Section 8.6 Continuité de service

En cas d'absence d'un utilisateur, toute mesure indispensable à la continuité du service peut être mise en œuvre qui ne contredise pas les règles décrites dans la présente charte et dans la PSSI de l'École polytechnique[4] (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 8.7 Confidentialité des données

Les utilisateurs doivent être extrêmement vigilants vis-à-vis des données considérées comme sensibles au sens de la politique de sécurité du système d'information et de communication.

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.

Le partage de données depuis un poste de travail est interdit (les utilisateurs doivent partager leurs données via un serveur de fichiers ou un serveur de gestion documentaire autorisés par le responsable de la sécurité du système d'information et de communication de l'École polytechnique, ou encore le porte-document du service de messagerie de l'École polytechnique ou d'un laboratoire).

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

ARTICLE 9 : RELATIONS AVEC LES SITES DISTANTS

Section 9.1 Connexion à un site distant

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

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

[4] La messagerie électronique de l'Ecole polytechnique fait exception (clôture puis destruction du compte de messagerie au-delà de la durée minimale définie à la section 4.8).

Section 9.2 Fonctionnement intègre du système d'information et de communication

Il est interdit de se livrer depuis des ressources informatiques appartenant à l'École polytechnique ou étant connecté aux réseaux informatiques de l'École polytechnique à des actes mettant sciemment en péril la sécurité ou le fonctionnement du système d'information, locaux ou distants, et des réseaux de télécommunications ou nuire à la réputation de l'École (exemple : redirection des noms de domaine institutionnels vers un site web non maitrisé).

Section 9.3 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 courriers courriels d'hameçonnage (phishing).

L'École polytechnique ne pourra être tenue responsable des dommages subis lors de telles divulgations d'informations.

L'administrateur se réserve le droit de bloquer les accès d'un utilisateur victime d'hameçonnage à des fins de protection du système d'information et de communication et d'audit, et ce pour toute la durée qu'il estime nécessaire.

Dans un objectif uniquement pédagogique, le RSSI ou son suppléant peuvent organiser des simulations d'attaque de type hameçonnage 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 10 : ECHANGES ELECTRONIQUES

Section 10.1 Devoir de réserve

Dans ses échanges, nul ne peut s'exprimer au nom de l'École polytechnique ou engager l'École polytechnique sans y avoir été dûment autorisé, ou sans que les fonctions qu'il exerce le prévoient.

Section 10.2 Règles de savoir-vivre

Chacun doit faire preuve de la plus grande correction à l'égard de ses interlocuteurs dans les échanges électroniques (mails, chats, réseaux sociaux, etc.).

Section 10.3 Responsabilité de l'utilisateur relative au contenu des échanges

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

Section 10.4 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'École polytechnique, du fait même du fonctionnement d'Internet.

Section 10.5 Publications sur un site Internet hébergé par l'École polytechnique

Il est rappelé que toute publication sur un site Internet hébergé par l'École polytechnique engage celle-ci, et son image.

ARTICLE 11 : EVOLUTION DE LA CHARTE

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

ARTICLE 12 : 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 poursuites en rapport avec les manquements constatés.

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.

[AQSSI] : Autorité Qualifiée de la Sécurité des Systèmes d'Information.

[CIL] : Correspondant informatique et libertés. Désigne le responsable chargé d'assurer l'application des dispositions des règlementations CNIL et GDPR à l'Ecole polytechnique

[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.

[Copyright] : Le copyright, souvent indiqué par le symbole ©, est, dans les pays anglo-saxons, l'ensemble des prérogatives exclusives dont dispose une personne physique ou morale sur une œuvre de l'esprit originale. Il désigne donc un ensemble de lois en application, notamment, dans les pays du Commonwealth et aux États-Unis ; Il diffère du droit d'auteur appliqué dans les pays de droit civil (tels que la France ou la Belgique par exemple).

[CSSI] : Correspondant des systèmes d'information. Désigne un groupe d'ASR

[DPO] : Data Protection Officer. Dénomination du CIL dans le cadre de la règlementation européenne GDPR. Le DPO a toutefois des attributions étendues en cohérence avec le nouveau cadre réglementaire.

[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 de l'Ecole polytechnique

[FTP] : File Transfer Protocol (protocole de transfert de fichier) est un protocole de communication destiné au partage de fichiers sur un réseau. Il permet, depuis un ordinateur, de copier des fichiers vers un autre ordinateur du réseau, ou encore de supprimer ou de modifier des fichiers sur cet ordinateur. Ce mécanisme de copie est souvent utilisé pour alimenter un site web hébergé chez un tiers.

[GEIDE] : Gestion Electronique de l'Information et des Documents de l'Entreprise.

[GDPR] : General Data Protection Regulation. Constitue le nouveau texte de référence européen en matière de protection des données à caractère personnel1. Il renforce et unifie la protection des données pour les individus au sein de l'Union européenne.

[INRIA] : Institut national de recherche en informatique et en automatique.

[LDAP] : Lightweight Directory Access Protocol est un protocole permettant l'interrogation et la modification des services d'annuaire.

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

[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

[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.

[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.