CHARTE D'UTILISATION DES RESSOURCES INFORMATIQUES DE L'ÉCOLE DES MINES DE SAINT-ÉTIENNE

(validée par le Comité Technique de l'EMSE le 21 février 2020)

La présente charte a pour finalité de contribuer à la préservation de la sécurité des systèmes d'information (SI) et de communication[1] de l'École des Mines de Saint-Étienne (ci-après dénommée « l'École ») et fait de l'utilisateur un acteur essentiel à la réalisation de cet objectif. Elle a également pour objet de sensibiliser les utilisateurs aux risques liés à l'utilisation des ressources informatiques[2] en termes d'intégrité et de confidentialité des informations traitées. Ces risques imposent le respect de certaines règles de sécurité et de bonne conduite. L'imprudence, la négligence ou la malveillance d'un utilisateur peuvent en effet avoir des conséquences graves de nature à engager sa responsabilité civile et/ou pénale ainsi que celle de l'École.

Le terme « **utilisateur** » désigne toute personne autorisée à accéder aux outils informatiques et aux moyens de communication de l'École et à les utiliser : personnel, stagiaires, intérimaires, personnels de sociétés prestataires, visiteurs occasionnels...

POURQUOI UNE CHARTE INFORMATIQUE ?

QUE CONTIENT-ELLE ?

La présente charte informatique définit les conditions d'accès et les règles d'utilisation des systèmes d'information (SI) 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 des Systèmes d'Information de l'École (DSI) ainsi que les mesures applicables en cas de non-respect de ces règles.

QUI CONCERNE-T-ELLE ?

Cette charte s'applique à toute personne utilisant les systèmes d'information (SI) et de communication :

- De l'École (réseau, matériel, services, Intranet…).
- Accessibles depuis le réseau de l'École (Internet).
- Associés aux activités de l'École (ressources informatiques des partenaires par exemple).

SUR QUELLES BASES LÉGALES SE FONDE-T-ELLE ?

Cette charte informatique est incluse dans le règlement intérieur de l'École. Elle est associée à la charte déontologique RENATER[3] (cf. annexe I), signée par l'École, et dont les règles d'usage sont reprises dans ce document.

Cette charte informatique se fonde également sur des textes de loi. Une annexe informative du dispositif légal en vigueur est jointe à la présente charte en annexe II.

---

[1] 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'organisation.

[2] Ressources informatiques : regroupe le matériel (ordinateurs, téléphone, copieurs, …), les logiciels, les procédures, les données et les fichiers informatiques.

[3] Le réseau informatique de l'École est relié à Internet via le Réseau national de télécommunications pour la technologie, l'enseignement et la recherche (RENATER).

DROITS ET OBLIGATIONS DES UTILISATEURS

CONDITIONS D'ACCÉS 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 son mot de passe.

L'accès aux SI de l'École est d'usage professionnel. Seuls les services présentant un lien direct et nécessaire avec l'activité professionnelle ont vocation à être utilisés.
Si une utilisation à titre privé des SI et donc des ressources informatiques est tolérée, c'est à la condition d'être raisonnable[4], licite et ne pas perturber le bon fonctionnement du service.

COMPTE INFORMATIQUE

Le droit d'accès aux SI de l'École via un compte informatique interne n'est accordé à un utilisateur qu'à condition qu'il remette au service gestionnaire de son dossier personnel (DPRH, DF, DRI, DSI) la déclaration (engagement individuel) stipulant qu'il a pris connaissance de la charte d'utilisation des ressources informatiques, après y avoir apposé sa signature.

La durée de vie du compte informatique est fonction du statut de l'utilisateur. Elle est précisée dans le catalogue de services[5] mis à disposition sur l'intranet.
À titre exceptionnel, le directeur de l'École ou son représentant peut accorder des prolongations du droit d'accès aux SI sur demandes motivées, formulées par écrit.

PROTECTION DES PERSONNES EN TERMES D'INFORMATIQUE ET LIBERTÉS

La loi n°78-17 du 6 janvier 1978 modifiée en 2004 relative à l'informatique, aux fichiers et aux libertés et le Règlement général sur la protection des données (RGPD) du 25 mai 2018 définit les conditions dans lesquelles des traitements de données à caractère personnel peuvent être effectués. Elle ouvre aux personnes concernées par les traitements un droit d'accès, et de rectification des données enregistrées sur leur compte.

L'École a désigné un Délégué à la protection des données (DPO) pour l'ensemble des campus de l'école. Ce dernier a pour mission de veiller au respect des dispositions de la loi n°78-17 du 6 janvier 1978 modifiée et du RGPD.

Tous les projets de traitement appelés à comprendre des données à caractère personnel, quelle que soit la procédure applicable, doivent être adressés à l'attention du Délégué à la protection des données
Le DPO est obligatoirement consulté par le responsable des traitements préalablement à la création de fichiers soumis aux dispositions de la loi informatique et libertés et du RGPD. Il recense dans un registre la liste de l'ensemble des traitements de données à caractère personnel de l'École au fur et à mesure de leur mise en œuvre. Cette liste est tenue à disposition de toute personne qui en fait la demande. Elle est également diffusée sur l'intranet de l'École[6].

Le DPO veille au respect des droits des personnes (droit d'accès, de rectification et d'opposition). En cas de difficultés rencontrées lors de l'exercice de ces droits, les personnes concernées peuvent saisir le correspondant (contact : cnil@mines-stetienne.fr).

RESPECT DES DROITS DE PROPRIÉTÉ ET DES LICENCES

Il est interdit aux utilisateurs des SI de réaliser des copies de tout logiciel mis à leur disposition, autre que ceux du domaine public et d'en faire un usage non conforme aux prescriptions de son auteur ou de la société qui le met à disposition, ainsi que de publier tout document protégé par les textes relatifs à la propriété littéraire et artistique.

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

---

[4] Le caractère raisonnable dépend du temps passé dans l'utilisation privative ; le caractère licite, des risques que cette utilisation fait courir à la sécurité des SI, de l'éventuelle mise en cause de la responsabilité de l'École et de son image.

[5] Le catalogue de services est consultable sur le site Services numériques de l'École : http://services-numeriques.emse.fr/catalogue-de-services

[6] Les déclarations CNIL sont consultables sur le site Services numériques de l'École : http://services-numeriques.emse.fr/cnil

RESPECT DU CARACTÈRE CONFIDENTIEL DES INFORMATIONS

Les utilisateurs ne doivent pas tenter :

- de lire, de copier, de modifier les fichiers d'un autre utilisateur sans son autorisation ;
- d'intercepter les communications privées entre utilisateurs, qu'elles se composent de courriers électroniques ou de dialogues directs ;
- d'utiliser de comptes autres que ceux pour lesquels ils bénéficient d'un droit d'accès ;
- d'effectuer des manœuvres qui auraient pour but de méprendre les autres utilisateurs sur leur identité ;
- de s'approprier ou de déchiffrer le mot de passe d'autres utilisateurs ;
- de limiter ou d'interdire l'accès aux systèmes d'information et de communication à des utilisateurs autorisés.

RESPONSABILITÉS DE L'UTILISATEUR

Chaque utilisateur 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 reconnaît également que toute violation des dispositions de la présente charte ainsi que, plus généralement, tout dommage créé à l'École ou à des tiers engagera sa propre responsabilité.

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

ADMINISTRATION DU SYSTÈME D'INFORMATION

OBLIGATIONS DE L'ÉCOLE

L'École fait bénéficier l'utilisateur (remplissant les conditions définies préalablement) d'un accès aux systèmes d'information et de communication de l'École. L'utilisateur dispose ainsi de nombreux services proposés par la DSI et encadrés par la politique de sécurité des systèmes d'information de l'Etat (PSSIE).

Un responsable de la sécurité des systèmes d'information (RSSI) a été nommé sur chacun des campus de Saint-Etienne et de Gardanne afin de garantir la sécurité, la disponibilité et l'intégrité du système d'information et des données.

La DSI assure le bon fonctionnement et la sécurité des réseaux, des moyens informatiques et de communication de l'École. Les membres de la DSI disposent d'outils techniques afin de procéder à la maintenance, aux investigations et au contrôle de l'utilisation des systèmes d'information et de communication mis en place, conformément à l'objet de cette charte d'utilisation des ressources informatiques.

COLLECTE ET TRAITEMENT DES INFORMATIONS

Pour des nécessités de maintenance et de gestion technique, d'analyses, de traçabilité, d'optimisation, de sécurité ou de détection des abus, l'utilisation des ressources informatiques et des services internet, ainsi que les échanges via le réseau peuvent être analysés et contrôlés dans le respect de la législation applicable et notamment de la loi informatique et libertés et du RGPD.

L'École est dans l'obligation légale (cf. annexe II) de mettre en place un système de journalisation des accès internet, de la messagerie et des données échangées de l'utilisateur.

La DSI s'engage à traiter 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 durée de connexion, en application de la loi en vigueur.

SYSTÈMES AUTOMATIQUES DE FILTRAGE

À titre préventif, des systèmes automatiques de filtrage, permettant de diminuer les flux d'information pour l'École et d'assurer la sécurité et la confidentialité des données, sont mis en œuvre. Il s'agit notamment du filtrage de sites Internet, de l'élimination ou de la mise en quarantaine des courriels non sollicités en fonction de leur dangerosité (spam, pièces attachées, virus, phishing…), du blocage de certains protocoles (peer to peer...).

SYSTÈMES AUTOMATIQUES DE TRAÇABILITÉ

La DSI opère sans avertissement les investigations nécessaires à la résolution de dysfonctionnements des systèmes d'information ou de l'une de ses composantes, qui mettent en péril son fonctionnement ou son intégrité. Elle s'appuie pour ce faire, sur des fichiers de journalisation (fichiers « logs ») qui recensent toutes les connexions et tentatives de connexions aux systèmes d'information. La DSI est le seul utilisateur de ces informations qui sont effacées à l'expiration du délai légal.

GESTION DU PARC INFORMATIQUE

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

À des fins d'assistance, les membres de la DSI peuvent accéder à distance au poste de travail de l'utilisateur. Cette intervention s'effectue avec l'autorisation expresse de l'utilisateur.

Dans le cadre de mises à jour et d'évolutions du système d'information, des mises à jours logicielles peuvent être réalisées automatiquement, généralement à la fermeture du poste de travail de l'utilisateur. Néanmoins la DSI peut être amenée à réaliser des mises à jour à tout heure selon le degré de sécurité associé. Les utilisateurs ont l'obligation d'accepter les mises à jour à l'extinction du poste de travail.

RESPONSABILITÉS - SANCTIONS

MESURES APPLICABLES EN CAS DE NON RESPECT DES RÈGLES

Le non-respect des règles établies ou rappelées par la Charte pourra donner lieu, indépendamment d'éventuelles sanctions pénales telles que prévues par les Lois en vigueur, aux sanctions suivantes :

Suspension de l'accès aux Services

L'utilisateur qui enfreint l'une des règles énoncées dans la présente charte encourt la suppression de son accès aux ressources informatiques et notamment au réseau RENATER.

La DSI peut ainsi en cas d'urgence (ou à la demande expresse du GIP RENATER) :

- limiter ou interrompre temporairement l'accès d'un utilisateur aux applications de l'École et au réseau internet, avec ou sans préavis selon la gravité de la situation,
- isoler ou neutraliser provisoirement toute donnée ou fichier manifestement en contradiction avec la présente charte ou qui mettrait en péril la sécurité des moyens informatiques.

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

Sanctions disciplinaires

Les sanctions disciplinaires concernant les personnels (fonctionnaires et contractuels) et les étudiants sont précisées dans le règlement intérieur de l'École.

RÈGLES GÉNÉRALES D'UTILISATION

UTILISATION RAISONNÉE

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

- ne pas mettre en péril la sécurité et l'intégrité des SI de l'École ;
- minimiser l'empreinte énergétique de l'École (exemples : extinction de son ordinateur, bonnes pratiques de la messagerie électronique) ;
- utiliser de manière efficace les outils et services mis à disposition.

UTILISATION DU MATÉRIEL INFORMATIQUE

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

- en réservant au préalable la salle ;
- en prenant soin du matériel mis à disposition.

L'utilisateur s'engage à prendre soin de tout matériel mis à sa disposition par l'École et à signaler tout dysfonctionnement constaté grâce à l'application des demandes d'intervention accessible depuis le portail applicatif[7] de l'École.

Le matériel informatique de l'École ne doit être utilisé que dans le cadre des missions validées par la direction, y compris le matériel nomade tels que les ordinateurs portables ou encore les téléphones mobiles (liste non-exhaustive), quel que soit le lieu d'utilisation.

En dehors des ordinateurs portables des élèves[8] requis pour suivre leur formation, l'apport de matériel personnel est toléré par la DSI, qui n'en garantit pas le support (maintenance, configuration, niveau de service…). L'usage de ce matériel ne doit pas altérer le fonctionnement ni la sécurité des systèmes d'information et de communication de l'École.

DONNÉES PERSONNELLES

Les courriels ne sont pas considérés comme personnels du simple fait de leur classement dans le répertoire «mes documents» ou dans un dossier identifié par les initiales de l'employé. Toutefois, un 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, les messages personnels doivent être identifiés comme tels, par exemple :

- en précisant dans leur objet «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 une 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 la messagerie.

Par défaut, les fichiers ont un caractère professionnel et l'École peut y accéder librement. Lorsque les fichiers sont identifiés comme personnels, l'École ne peut y accéder qu' :

- en présence de l'utilisateur ou après l'avoir prévenu ;
- en cas de risque ou évènement particulier, qu'il appartient aux différentes juridictions concernées d'apprécier.

MISE EN GARDE CONTRE L'EXTERNALISATION DES DONNÉES DE L'ÉCOLE

La DSI met tout particulièrement en garde les utilisateurs contre l'externalisation des données confidentielles, issues de l'administration, de la recherche ou de l'enseignement à 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 (cloud) n'appartenant pas à l'École et non approuvés par la DSI.

  → La DSI met généralement à disposition des outils similaires accessibles via le portail applicatif de l'École. La plupart de ces outils sont des services proposés pour la communauté enseignement recherche par le GIP RENATER.
- L'utilisation des « équipements nomades[9] » de l'École, ou l'enregistrement de données confidentielles sur du matériel personnel (connexions à des réseaux non sécurisés, matériel laissé sans surveillance…).

  Quand cela est techniquement possible, ils doivent faire l'objet d'une sécurisation particulière, au regard de la sensibilité des documents qu'ils peuvent stocker, notamment par chiffrement.

---

[7] Le portail applicatif de l'École est accessible à l'URL : http://portail.emse.fr

[8] Les ordinateurs portables des élèves font l'objet d'une convention spécifique.

[9] Tous les moyens techniques mobiles (ordinateur portable, imprimante portable, smartphone, clé usb…).

L'utilisation de smartphones pour relever automatiquement la 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 pendant quelques minutes, ils doivent donc être verrouillés par un moyen adapté de manière à prévenir tout accès non autorisé aux données qu'ils contiennent.

RÈGLES DE SÉCURITÉ

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

- Signaler à la DSI de l'École toute violation ou tentative de violation suspectée de son compte informatique et de manière générale tout dysfonctionnement.
- Choisir un mot de passe, au minimum de 8 caractères, combinant impérativement chiffres, lettres et caractères spéciaux. Par mesure de sécurité, l'utilisateur est dans l'obligation de le changer au moins une fois par an. Dans le cas contraire, et après plusieurs mails d'information, son compte sera temporairement bloqué.
- Ne jamais confier son identifiant/mot de passe.
- Ne jamais demander son identifiant/mot de passe à un collègue ou à un collaborateur.
- Ne pas masquer sa véritable identité.
- Ne pas usurper l'identité d'autrui.
- Ne pas modifier les paramétrages des matériels de l'École.
- Ne pas installer de logiciels sans autorisation et ne pas copier, modifier, détruire les logiciels propriétés 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 INTERNET/INTRANET

Les utilisateurs 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 conforme à la finalité du réseau RENATER. Une utilisation de cet accès à titre privé est tolérée, mais doit être 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 Direction des Systèmes d'Information, ayant délivré un droit d'accès. Elle s'engage à diffuser ces modifications aux utilisateurs concernés.

PAGES PERSONNELLES PROFESSIONNELLES

L'utilisateur des systèmes d'information et de communication ne doit pas stocker et mettre en consultation sur des serveurs de l'École des informations qui ne sont pas rigoureusement en rapport avec la mission de l'établissement. Toutefois, la création de pages personnelles « non professionnelles » grâce à des moyens et du matériel public est tolérée. Le contenu de ces pages ne doit poser aucun problème déontologique et doit respecter les obligations de l'utilisateur résultant de son statut et de son contrat. Ces informations doivent être régulièrement mises à jour.

PERSONNEL AYANT ACCÈS À DES DONNÉES CONFIDENTIELLES

Les personnels qui, 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 des SI de l'École.

Les personnels en charge des opérations de contrôle sont soumis à une obligation de confidentialité. Ils ne peuvent donc divulguer les informations qu'ils sont amenés à connaître dans le cadre de leur fonction, en particulier lorsqu'elles sont couvertes par le secret des correspondances ou relèvent de la vie privée de l'utilisateur, dès lors que ces informations ne remettent en cause ni le bon fonctionnement technique des applications, ni leur sécurité, ni l'intérêt du service.

ANNEXE I : CHARTE RENATER

Version: 2014

Charte déontologique RENATER

https://www.renater.fr/

(https://www.renater.fr/fr/telechargement,1392)

ANNEXE II : DISPOSITIONS LÉGALES APPLICABLES

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 226-13 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.

Règlement général sur la protection des données - RGPD

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016