CENTRALE NANTES

RÈGLEMENT INTÉRIEUR
DE L'ÉCOLE CENTRALE DE NANTES

- *Approuvé par le Conseil d'Administration en sa séance du 8 janvier 1996*
- *Modifié après approbation du Conseil d'Administration lors des séances du 30 mars 1998, du 10 mai 1999, du 27 janvier 2003, du 23 mai 2005, du 17 décembre 2007, 12 décembre 2016, du 23 octobre 2017, du 5 mars 2019, du 30 juin 2022, du 14 mars 2023, le 23 mai 2024 et le 12 décembre 2024.*

ANNEXE 3

CHARTE D'UTILISATION DES MOYENS INFORMATIQUES ET DES OUTILS NUMÉRIQUES

1. Préambule

Référencée dans le règlement intérieur, la charte informatique de l'École a pour but de :

- définir les règles d'utilisation de ses moyens informatiques ;
- définir les droits et devoirs des utilisateurs de ces moyens, ainsi que de l'École, fournisseur de ces moyens ;
- sensibiliser les utilisateurs aux problématiques de sécurité informatique.

Chaque utilisateur s'engage à respecter cette charte, dès lors qu'il utilise un moyen ou service informatique mis à disposition par l'École.

En cas de modification de la charte informatique, les utilisateurs sont prévenus par courrier électronique et sont réputés accepter tacitement l'ensemble des mises à jour.

2. Notions de « moyens informatiques », « utilisateur » & « compte informatique »

Sont qualifiés de « moyens informatiques » l'ensemble des équipements matériels informatiques fixes et mobiles (ordinateurs, tablettes, téléphones, imprimantes, etc.), l'ensemble des logiciels systèmes, support et d'application, ainsi que l'ensemble des dispositifs et services réseaux (Wi-Fi, Ethernet, box, cloud, etc.) déployés par l'École.

Est qualifié « d'utilisateur des moyens informatiques » : — tout membre des personnels permanents de l'École, — tout personnel des sociétés incubées dans l'incubateur Centrale-Audencia-Ensa qui a été agréé par convention, — tout étudiant inscrit à l'École, —tout personnel temporaire explicitement autorisé à cet accès par la direction de l'École.

Chaque utilisateur ainsi autorisé dispose d'un *compte informatique* personnel, auquel sont associés des droits d'accès qui lui sont propres (applications, services, dossiers partagés, etc.).

La signature de la présente charte est un préalable à l'ouverture dudit compte.

Pour se connecter à son compte, l'utilisateur doit saisir :

- un identifiant : attribué par l'École à l'utilisateur ;
- un mot passe : que l'utilisateur choisit et peut modifier lui-même.

La saisie de ces informations est un préalable d'accès à tout moyen informatique. Dans certains cas les identifiants ne sont pas requis car ils sont mémorisés par l'application à laquelle l'utilisateur accède de façon sécurisée.

3. Accès aux moyens informatiques

Les moyens informatiques connectables en réseau peuvent être interconnectés par le réseau de l'École, qui est lui-même connecté de façon sécurisée à Internet.

L'utilisateur peut ainsi accéder aux ressources dont les droits sont liés à son compte informatique, et ce via le réseau interne de l'école (Ethernet ou Wi-Fi), ou via une connexion Internet extérieure (le cas échéant avec VPN). La connexion peut être aussi bien établie via une box fibre/ADSL ou via le réseau de télécommunications « 3G/4G ».

La mise à disposition et l'utilisation de matériels mobiles propriétés de l'École (téléphones portables, PC portables, etc.) fait l'objet d'une charte spécifique.

4. Règles d'usage et de sécurité

L'usage des moyens informatiques de l'École doit être rationnel, loyal, et raisonnable, dans le respect des recommandations énoncées dans la présente charte et de la législation française en vigueur.

Tout utilisateur est responsable de son usage des moyens informatiques et des réseaux auxquels il a accès, et se doit de contribuer à la sécurité générale de l'École :

- il doit respecter l'intégrité et l'usage des moyens mis à disposition par l'École, et ne doit en aucun cas les dégrader. Il doit signaler tout problème de fonctionnement à la DSI ;
- il n'utilise que les seuls comptes pour lesquels il a reçu une autorisation. En aucun cas il ne fait part de ses codes d'accès à un tiers. Il lui est interdit d'utiliser un compte informatique ou des codes d'accès autres que les siens. Les identifiants et mots de passe ne doivent être communiqués à personne, y compris tout service de l'École. Note : aucun dépannage ne nécessite de connaître les mots de passe de l'utilisateur ;
- il choisit soigneusement ses mots de passe : difficiles à découvrir par autrui, tout en étant facile à retenir par lui (cf. recommandations et bonnes pratiques : https://www.ssi.gouv.fr/guide/mot-de-passe/) ;
- il doit verrouiller son poste de travail lorsqu'il le quitte, afin de ne pas laisser des ressources ou services accessibles à un tiers ;
- il est personnellement responsable de toute opération réalisée au moyen des codes d'accès dont il est détenteur.
- il est averti que seuls les ordinateurs gérés par la DSI font l'objet d'une sauvegarde régulière Il s'assure donc lui-même de la sauvegarde de ses données lorsque son poste n'est pas géré par la DSI ;
- il signale toute anomalie, constat de violation, tentative de violation ou soupçon de violation d'un système informatique aux administrateurs des moyens affectés, ainsi que à la DSI, au RSSI (Responsable de la Sécurité du Système d'Informations : rssi@ec-nantes.fr) et au FSD (Fonctionnaire Sécurité Défense : fsd@ec-nantes.fr) ;
- il est informé que le support utilisateurs DSI est le point de contact unique pour toute demande de suppression de compte, validation de compte, suppression de données, quota de messagerie, etc. De faux messages sont régulièrement envoyés par des pirates pour tenter de voler des données utilisateur, et tentent de se faire passer pour des messages envoyés par les services informatiques. Dans le doute, tout utilisateur doit impérativement contacter le support utilisateurs DSI (svp-dsi@ec-nantes.fr) et ne pas cliquer sur un lien dont il ignore la nature.

Concernant les matériels non gérés par la DSI, les règles suivantes doivent être respectées :

- toute connexion sur le réseau de l'École d'un équipement privé ou non identifié par la DSI doit faire l'objet d'une autorisation de la DSI ou du laboratoire concerné, qui peuvent requérir, pour cela, l'avis de l'autorité de cet utilisateur. Une fois cette autorisation obtenue, l'utilisateur s'engage à maintenir à jour son système et à le configurer dans les règles de l'art. En particulier, il doit se conformer aux règles de l'École, notamment pour lutter contre les virus et les attaques informatiques. Ces règles sont accessibles sur l'Intranet de l'École ;
- si l'activité de l'utilisateur requiert l'installation, le téléchargement ou l'utilisation de logiciels spécifiques non fournis par l'École, il doit s'assurer au préalable que leurs droits de licence ont été acquittés, que le site de leurs téléchargements est digne de confiance, puis obtenir l'autorisation de ces téléchargements auprès de la DSI ou du laboratoire concerné. L'installation de ces logiciels ne pourra être réalisée que sur un poste dont la gestion lui aura été confiée.

5. Conditions et limites d'utilisation des moyens informatiques de l'École pour un usage personnel

Les moyens informatiques de l'École sont à usage professionnel. Est donc considéré avoir un caractère professionnel de tout ce qui est fait, produit, réalisé ou consulté via un outil mis à disposition par l'École.

Toutefois l'utilisation à titre personnel de la messagerie, du stockage de fichiers, du téléphone et de l'accès à Internet via les moyens de l'École est tolérée sous réserve d'en faire un usage raisonnable, qui ne puisse altérer le bon fonctionnement de l'établissement, l'intégrité de son réseau informatique ou l'activité des agents de l'École.

Tout message envoyé ou reçu depuis une messagerie professionnelle est supposé avoir un caractère professionnel, sauf s'il est clairement identifié comme étant personnel par l'utilisateur. Pour être identifié comme étant personnel, un message devra être classé dans un dossier intitulé "PRIVE-PRIVATE".

Tous les fichiers présents sur un ordinateur de travail sont supposés être professionnels, sauf si clairement identifiés comme étant personnels par l'utilisateur. Pour être identifiés comme personnels, des documents doivent être classés dans un dossier intitulé "PRIVE-PRIVATE". L'intitulé "Mes documents", les initiales ou le prénom de l'utilisateur ne suffisent pas à donner un caractère personnel à un dossier.

6. Obligation de confidentialité

- toute tentative d'interception de communications entre tiers est interdite ;
- l'utilisateur n'a l'autorisation d'accéder qu'aux informations ou fichiers mis publiquement à disposition, ainsi qu'à ses informations ou fichiers propres. Il lui est interdit de prendre connaissance d'informations ou de fichiers réservés à l'usage d'autres utilisateurs, même si ces éléments ne sont pas protégés. Toute violation de la présente obligation est susceptible d'engager la responsabilité civile ou pénale de son auteur ;
- il est tenu à la discrétion et au secret professionnel concernant toute information relative au fonctionnement interne de l'ECN et de ses ressources informatiques ;
- il est tenu de prendre les mesures de protection des données nécessaires au respect des engagements de confidentialité pris par l'ECN vis-à-vis de tiers ;
- l'Intranet de l'établissement est un espace de diffusion d'informations à usage interne.

7. Obligations relatives à la propriété intellectuelle

L'utilisation de tout logiciel (source ou binaire) et plus généralement de tout document (fichier, image, son, etc.) doit respecter la loi sur la propriété intellectuelle, les recommandations fixées par les détenteurs de droits et les engagements pris par l'ECN (contrats de licences par exemple). En particulier :

- il est strictement interdit d'effectuer des copies de logiciels commerciaux pour quelque usage que ce soit, hormis une copie de sauvegarde dans les conditions prévues par le code de la propriété intellectuelle ;
- l'installation de tout logiciel ne peut se faire que dans le respect de la législation en vigueur, le respect des préconisations de l'auteur et de l'éditeur, et des recommandations de la DSI. Il est également subordonné au paiement de son droit d'utilisation ;

il est interdit de contourner les restrictions d'utilisation d'un logiciel.

8. Analyse et contrôle de l'utilisation des ressources informatiques par l'École

Pour des raisons légales et des nécessités de sécurité, de maintenance et de gestion technique, les données d'utilisation des ressources matérielles, logicielles et réseaux sont enregistrées dans des fichiers stockés puis archivés et conservés pendant leurs durées réglementaires. Ces données peuvent être exploitées pour retrouver l'origine d'un dysfonctionnement, d'un comportement malveillant ou d'un usage inadapté.

Les procédures mises en œuvre sont conformes à la législation française et européenne, notamment au RGPD (Règlement Général sur la Protection des Données personnelles) et aux décisions s'appliquant depuis la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

9. Données à caractère personnel

Les dispositions de l'École relatives à l'application du Règlement Général sur la Protection des Données personnelles (RGPD) sont diffusées à l'ensemble des utilisateurs de l'École, et sont consultables sur son Intranet.

10. Administration des Systèmes d'Information

(SI : Système d'Information)

Par la suite, le terme « administrateur SI » désigne une personne qui, dans le cadre de sa charge et de ses missions, agit dans le but d'administrer, d'assurer le fonctionnement et l'exploitation d'un ou plusieurs composants de traitement de l'information, matériels ou logiciels (outils, réseaux, bases de données, messagerie, ...) de l'établissement ou des entités qui le composent.

Un administrateur SI a pour mission d'assurer le bon fonctionnement et la sécurité des ressources du Système d'Information placées sous sa responsabilité, dont notamment les serveurs, les équipements réseaux, les équipements de sécurité, les applications, les bases de données et les postes de travail.

Pour l'exécution de sa mission, l'administrateur SI dispose de droits d'accès techniques susceptibles de lui permettre l'accès à des informations, tels que des courriels, des fichiers, des données de connexion (confidentielles ou non), et de façon générale à des données à caractère privé ou professionnel, dont il n'est ni le destinataire, ni l'auteur, ni le propriétaire.

L'administrateur SI est tenu au secret professionnel, et soumis à l'obligation de discrétion professionnelle. Il exerce ses missions dans le respect des prescriptions règlementaires régissant son statut, excluant de fait toute utilisation de ses droits d'accès à des fins personnelles. De même, il n'utilise pas ses droits pour transmettre des données dont le traitement fait l'objet d'une procédure en place, et ainsi se substituer à l'entité en charge de ces données.

Droits de l'administrateur SI

Dans le cadre de ses missions, un administrateur SI a le droit :

- d'interrompre le fonctionnement de tout équipement, logiciel ou matériel, qui compromettrait la sécurité ou le bon fonctionnement du SI ;

- d'utiliser des données de connexion (ce qui peut impliquer la découverte d'informations privées) à des fins de diagnostic, de vérification, de métrologie, de statistiques ou en cas d'anomalie ou d'incident;
- d'intercepter ou interdire tout flux informatique (web, courriel, transfert de fichiers, téléphonie, vidéo, etc.) présentant des risques potentiels pour la sécurité (virus par exemple), ou dérogeant à la présente charte informatique ;
- de prendre les mesures adéquates afin de prévenir tout risque de sécurité tel que virus, intrusion ou vol de données, destruction de données ou contournement de la politique de sécurité.

Devoirs de l'administrateur SI

Dans le cadre de ses missions, un administrateur SI :

- ne prend pas connaissance de données d'utilisateurs identifiées comme personnelles - sauf ponctuellement, sur accord formel de l'utilisateur lui-même - et n'autorise personne à y accéder, sauf cas particuliers prévus par la loi ;
- respecte scrupuleusement la confidentialité des informations auxquelles il a accès et met en œuvre des mesures visant à assurer leur non divulgation ;
- collabore avec le délégué à la protection des données (DPO) pour que la mise en œuvre des traitements respecte la réglementation sur la protection des DCP (données à caractère personnel). Il contribue à la disponibilité, la confidentialité et l'intégrité des données concernées et alerte le DPO de tout incident en la matière ;
- collabore avec les autres administrateurs SI afin de garantir un traitement global de l'information, dans le respect de la présente charte ;
- informe le Responsable de la Sécurité des Systèmes d'Information (RSSI) de tout incident de sécurité dont il pourrait avoir connaissance ;
- n'utilise ses droits d'accès qu'exclusivement pour les activités et les besoins directement liés à ses missions, et en aucun cas à des fins personnelles ;
- agit dans le sens d'une meilleure sécurité et dans l'intérêt de l'établissement.

Engagements de l'administrateur SI

L'administrateur SI s'engage à respecter en toutes circonstances la législation en vigueur et le règlement intérieur de l'établissement, incluant les dispositions de la présente charte.

En cas de non-respect, l'administrateur SI sera tenu pour responsable de ses actes et pourra encourir des sanctions disciplinaires, civiles ou pénales.

11. Continuité de service en cas d'absence d'un salarié

En cas d'impossibilité d'un salarié (en cas d'arrêt maladie par exemple) de fournir les informations, dont il dispose ou auxquelles il a accès dans des systèmes informatiques, qui sont nécessaires à la continuité de service des activités de l'établissement, le directeur de l'établissement peut à titre exceptionnel autoriser l'accès à ces informations ou systèmes informatiques, par des personnes nominativement désignées, de façon strictement encadrée.

Cette autorisation formalisée par écrit, et portée à la connaissance du salarié dont l'absence est susceptible de rompre la continuité de service, inclura les éléments suivants :

- identité du salarié absent ;
- rappel du contexte (arrêt maladie de l'agent, etc.) ;
- données ou systèmes accédés ;
- finalités au titre de l'article 6.1.e du RGPD ;
- périmètre des données accédées (ex : accès aux seuls messages professionnels) ;
- liste nominative et fonctions des personnes ayant cet accès ;
- présence obligatoire du DPO (Délégué à la Protection des Données Personnelles) ;
- période(s) pendant laquelle(lesquelles) ces accès sont autorisés.

Un PV sera rédigé, et tenu à disposition du salarié, dans lequel seront consignées les modalités de déroulement de ces consultations, les éléments consultés, et le cas échéant les actions entreprises.

12. Respect de la législation

Il est rappelé que tout utilisateur doit respecter l'ensemble de la législation applicable, notamment dans le domaine de la sécurité informatique et des données personnelles. Ces textes sont actualisés en permanence et peuvent être consultés sur les sites de la CNIL (www.cnil.fr) et de LEGIFRANCE (www.legifrance.gouv.fr), qui diffuse gratuitement l'essentiel du droit français.

13. Sanctions encourues

En cas d'infraction à la présente charte ou aux dispositions réglementaires en vigueur, les droits d'accès autorisés par l'École peuvent être suspendus ou définitivement retirés. Le non-respect d'une de ces règles est susceptible d'entraîner des mesures disciplinaires internes à l'établissement.

Toute personne ayant enfreint la loi s'expose à des poursuites judiciaires. Il est donc rappelé à l'utilisateur que ses actions peuvent avoir des conséquences juridiques lourdes à la suite de comportements non autorisés.