Charte du bon usage
des systèmes d'information
à l'École normale supérieure.
13 juin 2016

1.- Domaines d'application :

Cette charte, rédigée dans le cadre de la Politique de Sécurité des Systèmes d'Informations (PSSI) de l'Ecole, s'applique à toute personne utilisant les systèmes et réseaux informatiques situés sur les sites de l'École normale supérieure, les systèmes informatiques auxquels il est possible d'accéder à partir de l'École ainsi que les systèmes informatiques d'organismes extérieurs à l'École, mentionnés dans le contrat d'études d'un élève ou ayant passé une convention avec l'École.

2.- Autorisation d'accès aux systèmes et réseaux informatiques :

2.1. L'utilisation des ressources informatiques à l'École est soumise à autorisation préalable, concrétisée par l'ouverture d'un compte ou le droit de connecter un ordinateur sur le réseau.

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

2.3. L'utilisation des systèmes d'information est limitée à des activités de recherche et d'enseignement, de développements techniques, de transferts de technologies, de diffusion d'informations scientifiques, techniques et culturelles, d'expérimentation de nouveaux services présentant un caractère d'innovation technique, mais également toute activité administrative ou de gestion liée à ces activités. Sauf autorisation préalable, ces moyens ne peuvent être utilisés pour des projets faisant l'objet d'un financement extérieur à l'École.

2.4. L'École se réserve le droit de retirer à tout moment cette autorisation, et ce, sans préavis.

2.5. Cette autorisation prend fin lors de la cessation de l'activité qui l'a justifiée. En ce qui concerne les élèves et étudiants, elle prend fin dans le délai d'un an maximum après la fin de la scolarité, sauf raison exceptionnelle validée par le Directeur de l'École.

2.6. Lors de la fermeture de son compte, l'intéressé peut obtenir copie du contenu de celui-ci, sauf cas particuliers (clause de propriété, de confidentialité, etc.). L'utilisateur est responsable avant son départ de la destruction de ses données privées.

2.7. Toute connexion de matériel personnel est soumise à autorisation et se fait dans le cadre d'usages professionnels et des règles de sécurité de l'École et de ses laboratoires et départements. L'École ne peut être tenue pour responsable en cas de vol ou de dégradation des équipements appartenant aux personnels, élèves, étudiants ou visiteurs.

2.8. Dans les espaces privatifs (internat, logement), chacun est responsable du trafic relatif à sa connexion.

3.- L'administrateur-système :

Sont administrateurs-système les personnes ayant été désignées pour installer et gérer les machines. Ils sont en charge d'assurer la meilleure marche possible du système pour tous.

3.1. L'administrateur-système est soumis dans l'exercice de ses fonctions à un devoir de confidentialité. Pour assurer le bon fonctionnement et la sécurité du système informatique, il peut procéder aux investigations nécessaires. Il est tenu de ne pas divulguer les informations acquises par ces recherches sauf dans le cas prévu au 3.2.

3.2. En particulier il peut explorer les fichiers des utilisateurs et en faire connaître des extraits à la Direction des départements et de l'École lorsqu'une telle recherche est rendue nécessaire par le constat d'actes de piratage.

3.3. Il peut aussi générer et consulter tout journal d'événements, et enregistrer des traces, si besoin est. La liste exhaustive de ces journaux peut être consultée par simple demande auprès des administrateurs système.

Il peut générer des statistiques, pour la bonne gestion : optimisation, sécurité, détection des abus.

3.4. L'administrateur-système peut réaliser des sauvegardes de certains disques, y compris ceux hébergeant les données des utilisateurs et le courrier électronique.

3.5. L'administrateur peut intercepter ou interdire tout flux informatique (Web, courriel, transfert de fichiers, téléphonie, vidéo, etc.) présentant des risques pour la sécurité (virus par exemple), ou hors charte.

3.6. Les administrateurs sécurité peuvent procéder à toute recherche préventive de faille sur les machines, personnelles ou non, branchées sur le réseau interne. Ils peuvent déconnecter, physiquement ou logiquement, une machine en cas de suspicion.

4.- Règles générales de sécurité :

Tout utilisateur est responsable de l'utilisation qu'il fait des ressources informatiques dans l'École. Il doit donc, à son niveau, contribuer à la sécurité. En particulier :

4.1. Tout utilisateur doit choisir des mots de passe sûrs respectant les recommandations de l'administrateur-système, et l'administrateur peut en tester la robustesse. Ces mots de passe doivent être gardés secrets, ne doivent pas être écrits, ne doivent pas être enregistrés dans des systèmes (hors cryptage fort), et en aucun cas être communiqués à des tiers. À la demande des administrateurs-système, ils doivent être changés.

4.2. Les utilisateurs ne doivent pas utiliser des comptes autres que ceux pour lesquels ils ont reçu une autorisation. Ils doivent s'abstenir de toute tentative de s'approprier ou de déchiffrer le mot de passe d'un autre utilisateur.

4.3. L'utilisation ou le développement de programmes mettant sciemment en cause l'intégrité des systèmes informatiques de l'École ou des réseaux nationaux ou internationaux sont interdits.

4.4. Tout constat de violation, tentative de violation ou soupçon de violation d'un système informatique doit être signalé aux responsables sécurité de l'École.

4.5. Les utilisateurs ne doivent pas abandonner de machine sans s'être préalablement déconnectés.

4.6. Les utilisateurs doivent s'abstenir de toute tentative de falsification d'identité.

4.7. Les utilisateurs ne doivent pas ajouter d'équipements (ordinateur, imprimante, commutateur réseau, point de connexion wifi,...) sans autorisation. La connexion temporaire d'un ordinateur à un réseau "invité" est autorisée dans le respect des règles afférentes à ces réseaux.

4.8. Les utilisateurs s'engagent à ne pas exploiter les éventuels trous de sécurité, anomalies de fonctionnement, défauts de configuration. Ils doivent les signaler à l'administrateur-système, et ne pas en faire la publicité. L'administrateur peut toutefois choisir de ne pas apporter de correction, si la correction n'est pas disponible ou est considérée comme induisant d'autres problèmes.

4.9. Les utilisateurs évitent au mieux l'introduction et la propagation de virus sur les moyens informatiques.

4.10. Les utilisateurs doivent veiller à la sécurité de leurs données professionnelles, y compris leur courrier électronique, en terme de confidentialité, intégrité et disponibilité. Cela implique de s'assurer qu'une sauvegarde est effectuée à une fréquence adaptée au besoin et que leur lieu de stockage est pérenne. Le chiffrement est obligatoire dans le cas d'usage d'informatique nomade (ordinateurs portables, clés USB, PDA, disques externes, etc.).

L'usage de services externes (espace disques, messagerie, bureautique, etc.) et les serveurs de données (Web, ftp, etc.) ne présentant pas de garantie contractuelle de confidentialité, intégrité et disponibilité est interdit, sauf autorisation expresse et mise en oeuvre de mesures de protection adéquates.

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).

4.11. Les utilisateurs doivent respecter les règles définies par les autorités de tutelle (exemple : circulaire Guyon du 4 mai 2000 à propos du P2P, recommandation CNRS du 10 août 2005 à propos de Skype, recommandations CNRS du 17 avril 2008 pour l'usage des services gratuits sur Internet, circulaire JM.Voltini du 16 janvier 2011 sur le chiffrement des disques, etc.).

4.12. En règle générale, un utilisateur doit être vigilant et signaler aux administrateurs-système toute anomalie, et se conformer à leurs consignes.

4.13. Les utilisateurs doivent déclarer tout vol de matériel informatique, personnel ou professionnel, afin de prendre rapidement les mesures appropriées.

4.14. Les utilisateurs doivent être vigilants lors de connexions à des réseaux sans fil peu sécurisés, notamment les lieux publics.

5.- Utilisation des ressources communes :

5.1. Tout utilisateur s'engage à utiliser correctement les ressources mises à sa disposition : mémoire à ne pas saturer, espace disque, bande passante des réseaux, imprimantes, etc. Par exemple, les chaînes de courrier électronique sont interdites.

5.2. Tout utilisateur s'engage à respecter les ressources qui ne lui sont pas mises à sa disposition même si elles lui sont accessibles (imprimante par exemple).

6.- Respect de la propriété intellectuelle :

6.1. La reproduction des logiciels commerciaux autre que pour l'établissement d'une copie de sauvegarde est interdite.

6.2. Il est interdit d'installer sur tout système utilisé dans l'École un logiciel, une fonte ou tout autre document en violation des copyrights et licences associés. Les clauses de redistribution des logiciels libres doivent être respectées.

6.3. Les logiciels professionnels mis à disposition par l'École sur des machines personnelles doivent être supprimés lors du départ de l'Ecole.

6.4. L'usage des ressources documentaires doit être conforme au contrat de mise à disposition de l'éditeur validé par l'Ecole. Notamment, le télédéchargement massif et systématique de ressources documentaires par l'intermédiaire d'un robot ou de tout autre logiciel est interdit.

7.- Respect de la confidentialité des informations :

7.1. 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.

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

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

7.4. Les traitements de données nominatives doivent rester confidentiels et dans le respect des déclarations CNIL effectuées.

7.5. En cas d'absence d'un utilisateur, toute mesure indispensable à la continuité du service peut être mise en oeuvre.

7.6. Les utilisateurs doivent être extrêmement vigilants vis à vis des données considérées comme sensibles au sens de la politique de sécurité des systèmes d'informations. 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. Lors de consultations d'informations sensibles, les utilisateurs doivent être vigilants quant aux traces laissées : historique de navigateurs, mots de passe, caches, etc.

8.- Relations avec les autres sites informatiques :

8.1. Il est interdit de se connecter ou d'essayer de se connecter sur un autre site sans y être dûment autorisé. L'accès aux services anonymes (Web, ftp, etc.) est autorisé.

8.2. Il est interdit de se livrer depuis des systèmes appartenant à l'École ou étant connecté au réseau informatique de l'École à des actes mettant sciemment en péril la sécurité ou le fonctionnement des systèmes d'informations, locaux ou distants, et des réseaux de télécommunications.

8.3. Les utilisateurs doivent être vigilants lors de toute saisie d'informations personnelles sur Internet, notamment avec la multiplication des courriers d'hameçonnage (*phishing*). L'Ecole ne pourra être tenue responsable des dommages subis lors de telles divulgations d'informations.

8.4 : Les utilisateurs se connectant en utilisant leur identifiant Eduroam ENS doivent respecter les règles imposées par le site d'accueil.

8.5 : Les utilisateurs externes utilisant les connexions Eduroam proposées par l'ENS s'engagent à respecter cette charte et plus généralement la PSSI de l'ENS.

9.- Échanges électroniques :

9.1. Dans ses échanges, nul ne peut s'exprimer au nom de l'École ou engager l'École sans y avoir été dûment autorisé.

9.2. Chacun doit faire preuve de la plus grande correction à l'égard de ses interlocuteurs dans les échanges électroniques.

9.3. Compte tenu de la valeur juridique d'un courriel, chacun doit être vigilant sur le contenu des messages électroniques et s'assurer de leur conservation.

9.4. Il est rappelé qu'aucune garantie de bonne transmission ne peut être apportée aux courriers qui sont émis ou réexpédiés hors de l'École.

9.5. Il est rappelé que toute publication sur un site Internet hébergé dans l'École engage celle-ci.

9.6. L'usage à titre non professionnel d'une adresse de l'École (forums, blogs, ou toute autre publication sur Internet) doit être évité.

10.- Évolution de cette charte

Cette charte est consultable sur les serveurs Internet de l'École, et elle est susceptible de modifications en fonction des évolutions techniques. Seule la dernière version française fait foi, les versions en langue étrangère n'ont qu'une valeur informative.

11.- 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, internes à l'École (disciplinaires), civiles ou pénales (lois du 6 janvier 1978, du 6 août 2004, du 4 juillet 1985, du 5 janvier 1988, du 4 août 1994, et du 30 décembre 1990 (modifiée le 26 juillet 1996, et le décret du 17 mars 1999), 15 novembre 2001, 21 juin 2004 (et le décret 2011-219 du 25 février 2011), 3 août 2006, 12 juin 2009, 28 octobre 2009, 14 mars 2011).