

# Charte sécurité informatique - 42

42 propose, au travers de certains projets, un enseignement lié à la sécurité des technologies de l'information.

La présente Charte définit les règles d'usage qui s'imposent à tous les participants à ces projets. Elle constitue une dérogation temporaire et locale aux règles en vigueur sur l'utilisation courante du parc informatique de l'école. Elle s'adresse à tous les étudiants de 42 impliqués dans un projet lié à de la sécurité informatique, et ne s'applique que dans le cadre de ce type de projet. Dans tous les autres cas, les élèves doivent suivre les règles classiques en vigueur.

Cette charte est réputée connue de tous, avec ses autorisations et ses limites. Elle s'applique automatiquement à tout projet impliquant de la sécurité informatique. Tout étudiant réalisant un tel projet doit s'y conformer pleinement, sans restriction, et la faire respecter par tous. Contrevenir aux règles de cette charte peut aboutir à un renvoi de l'école ainsi que des poursuites judiciaires.

## Intérêt public

- Les élèves sont tenus de reconnaître et respecter les droits des individus et groupes d'individus à la confidentialité de leurs informations.
- Les élèves ont le devoir d'encourager les efforts entrepris pour faire progresser l'information concernant les problématiques liées à la sécurité informatique et doivent communiquer à l'Ecole tout renseignement important concernant les luttes qui en découlent. C'est à l'Ecole seule de décider si l'alerte doit ou non être transmise publiquement.

## Responsabilités par rapport aux Lois

- Les élèves sont tenus de respecter les contraintes légales telles que les copyrights, les brevets et les accords de licence. Il s'agit de ne faire circuler sur le réseau que des informations légales vis-à-vis des lois.
- Les élèves sont tenus de respecter les contraintes déontologiques qui ne sont pas toujours soumises à la loi.
- Les élèves sont tenus de reconnaître et de respecter les droits à la propriété intellectuelle.
- Les élèves sont tenus de se maintenir au courant des dispositions légales applicables à leur situation personnelle et professionnelle et de s'y conformer.
- Aucune attaque physique ne sera tolérée.

## Droits et Devoirs

- La modification irrévocable de données informatiques est formellement interdite. Il en résulte que chaque groupe devra fournir une documentation complète sur les fonctionnalités de leur projet ainsi que les moyens de prévenir tout dégât occasionnel. Ces mesures visent à exercer un contrôle pour assurer une réponse rapide et efficace en cas de problèmes.
- Les élèves s'engagent à n'intenter aucune action qui puisse discréditer l'école. Dans le cadre particulier des projets de sécurité informatique, les élèves doivent obtenir l'accord de l'école pour utiliser et communiquer avec son nom.
- 42 se réserve le droit d'apporter des modifications à la présente charte. Les élèves sont tenus de la parcourir régulièrement. Toute altération sera reportée sur le forum ou par mail.
- Le parc informatique mis à la disposition des étudiants appelle à une utilisation strictement professionnelle conforme à sa finalité : enseignement, recherche et développement, information.
- Il est strictement interdit de donner accès au réseau informatique 42 à des personnes extérieures à l'école, sauf accord préalable de l'école.

- Tout étudiant est par la présente charte informé et accepte que les administrateurs du parc informatique procèdent à des contrôles de la bonne utilisation de celui-ci, ainsi qu'au respect de cette charte et/ou des règles en vigueur.
- Aucune attaque physique ne sera tolérée.

### **Restrictions**

- La diffusion publique d'informations relatives à une faille d'un système informatique, même à des fins bénévoles comme l'alerte aux victimes potentielles de cette faille, est soumise à approbation de l'école. On entend ici par "publique" tout ce qui sous-tend un cadre extérieur aux participants d'un projet soumis à cette charte.
- Il est interdit d'écrire, de conserver ou de diffuser des codes destructeurs. Dans le cas présent, la volonté de nuire de l'auteur n'aura pas à être démontrée.
- Aucune attaque physique ne sera tolérée.

### **Cibles autorisées et limite de temps**

- Chaque projet dispose de ses propres contraintes. La Charte pose le cadre général de ces restrictions, pour tout le reste, c'est le sujet qui prévaut (on trouvera par exemple la liste des actions qui peuvent ou ne peuvent être effectuées, le réseau cible et les éventuelles dates pendant lesquelles il est mis à disposition des étudiants).
- Toute action portée à l'encontre de cible non mentionnée sur le sujet entraînera de sévères sanctions.
- Si des dates de départ et de fin de chaque projet sont fixées par le sujet ou l'intranet, il est strictement interdit d'effectuer une action sur le réseau cible en dehors de ces dates.

### **Environnement de travail et garantie de confinement**

- Pour faire des tests et construire le projet final, les élèves peuvent reconstituer un environnement de travail semblable à celui offert par 42. Cet environnement est tenu aux mêmes règles de la présente charte et doit rester un environnement informatique sain (c'est à dire pouvoir attester de sa sécurité et de son parfait contrôle).
- Pendant l'exercice d'un projet, la garantie de confinement doit être parfaitement assurée. Avant de pouvoir entamer une action (de quelque nature que ce soit : déployer un virus, intercepter un flux TCP, etc..), chaque programme doit impérativement suivre toute demande de contrôle préalable de l'action à venir, citée par le sujet ou le barème, ou émanant de tout autre autorité de l'école (confiner dans une VM, couper le réseau, ne pas exécuter en root, etc..). Si ces vérifications échouent, il est interdit de poursuivre. Tout groupe n'ayant pas respecté cette règle devra répondre de lourdes sanctions.