# CHARTE DES ADMINISTRATEURS DES RESSOURCES INFORMATIQUES DE L'ENSAIT

Annexe 1.1 du règlement intérieur de l'ENSAIT

Les personnels membres de la Direction des Systèmes d'Information (DSI) exercent des missions indispensables à la conduite des activités de l'ENSAIT. Ces personnels sont appelés « administrateurs du système d'information » et disposent de droits d'accès étendus. Dans l'exercice de leur fonction, ils peuvent être amenés à accéder à des informations ou des données d'autres utilisateurs présentant un caractère confidentiel. Ils effectuent également des actions sensibles. Tout action de ce type mal exécutée peut entraîner de graves conséquences telles que l'indisponibilité de certaines applications, l'altération voire la destruction ou la compromission d'informations importantes.

En raison de leurs prérogatives, ces personnels ont un rôle essentiel, requérant responsabilité et discrétion. Leur démarche se doit d'être impartiale, leurs interventions ne doivent pas outre passer leurs attributions ni relever d'actions effectuées pour leur propre compte ou par intérêt personnel. Il convient donc de fixer les règles, en particulier de déontologie, à respecter.

La présente *Charte des administrateurs des ressources informatiques de l'ENSAIT* est destinée à préciser les droits et les devoirs de toutes personnes chargées de la gestion d'éléments du système d'information de l'ENSAIT. Il s'agit d'une charte déontologique, elle n'a pas pour but de décrire les métiers d'administrateurs systèmes, réseaux ou systèmes d'information.

Cette charte fait référence à la Charte d'utilisation des ressources informatiques annexée au Règlement intérieur de l'ENSAIT, ainsi qu'à la Charte déontologique de RENATER mentionnée dans cette charte d'utilisation.

## ARTICLE 1 – DEFINITIONS ET ACRONYMES

**Système d'information (SI) :** Le Système d'Information est un ensemble de ressources et de dispositifs permettant de collecter, stocker, traiter et diffuser les informations nécessaires au fonctionnement de l'ENSAIT. Le système d'information ne doit pas être confondu avec le système informatique.

**Système Informatique :** Le Système Informatique est un sous-ensemble du système d'information. Il regroupe l'ensemble des moyens informatiques nécessaires au traitement de l'information : ordinateurs, programmes, réseau, logiciels, etc.

**Administrateur du Système d'Information :** L'administrateur du système d'information est toute personne, employée ou non par l'ENSAIT, à laquelle a été confiée la responsabilité permanente ou ponctuelle d'un élément du système d'information : une personne à qui a été conférée une telle responsabilité sera désignée par le terme « administrateur ».

L'ensemble des éléments sur lesquels s'exerce cette responsabilité constitue le périmètre d'activité de l'administrateur.

L'administrateur est une personne possédant une compétence reconnue pour gérer tout ou partie des systèmes d'information ou de télécommunications. Il possède des droits étendus dans la limite des nécessités de ses missions quant à l'utilisation et à la gestion du système d'information. Dans le cadre

de son activité, il pourra être amené à avoir accès aux informations des autres utilisateurs, informations parfois confidentielles.

**Responsable fonctionnel de système informatique :** Le responsable fonctionnel est la personne en charge de l'administration de l'entité (directeur de service, responsable administratif…), et par extension, il a la responsabilité fonctionnelle d'une partie du système d'information.

**Responsable Sécurité du Système d'Information (RSSI) :** Le RSSI définit et développe la politique de sécurité de l'information de l'ENSAIT. Il est garant de sa mise en œuvre et en assure le suivi.

**Politique de Sécurité du Système d'Information (PSSI) :** La PSSI est formalisée dans un ensemble de documents élaborés à partir d'une analyse de risques et débouchant sur une liste de mesures retenues. Ces documents sont confidentiels puisqu'ils dévoilent les aspects critiques et/ou fragiles du Système d'Information. Ils sont donc diffusés en fonction des besoins de leur destinataire. Dans le présent document les « *mesures de sécurité de la PSSI* » désigne le sous ensemble des mesures de SSI connues des personnes dont il est question.

## ARTICLE 2 – DROITS ET DEVOIRS DES ADMINISTRATEURS

Dans le cadre strict des missions qui lui sont confiées et du respect des mesures de sécurité de la PSSI, tout administrateur a le droit :

- D'être informé par sa hiérarchie des implications légales de son travail, en particulier des risques qu'il court dans le cas où un utilisateur du système dont il a la charge commet une action répréhensible.
- De mettre en place des moyens permettant de fournir des informations techniques d'administration des éléments du système d'information à sa charge (métrologie, surveillance…).
- De mettre en place toutes procédures appropriées pour vérifier la bonne application des règles de sécurité de la PSSI, en utilisant des outils autorisés.
- D'accéder, sur les systèmes qu'il administre, à tout type d'informations, uniquement à des fins de diagnostic et d'administration du système, en respectant scrupuleusement la confidentialité de ces informations, en s'efforçant de ne pas les altérer (tant que la situation ne l'exige pas).
- D'établir des procédures de surveillance de toutes les tâches exécutées sur le système dont il a la responsabilité, afin de déceler les violations ou les tentatives de violation de la présente charte et de la Charte d'utilisation des ressources informatiques, sous l'autorité de son responsable fonctionnel et en relation avec le RSSI.
- De prendre des mesures conservatoires, sans préjuger des sanctions résultant des infractions aux différentes chartes, quand il estime qu'une urgence impose de protéger l'intégrité, la disponibilité ou la confidentialité d'un service du système d'information.
- De ne pas intervenir sur un composant hors du système d'information (interne ou externalisé) de l'ENSAIT et hors d'un système d'information confié à l'ENSAIT par convention avec un partenaire, sauf à l'isoler du réseau de l'ENSAIT en cas de besoin.

Tout administrateur a le devoir :

- De respecter les dispositions légales et réglementaires concernant le système d'information[1] et pour se faire, de se renseigner, si nécessaire, auprès de sa hiérarchie, du RSSI, du service juridique et le délégué à la protection des données de l'ENSAIT.
- De respecter la confidentialité des informations auxquelles il accède lors de ses tâches d'administration ou lors d'audit de sécurité, quel qu'en soit le support (numérique, écrit, oral) et en particulier :
  - Les données à caractère personnel contenues dans le système d'information.
  - Les fichiers utilisateurs.
  - Les flux sur les réseaux.
  - Les courriers électroniques.
  - Les mots de passe.
  - Les sorties imprimantes.
  - Les traces des activités des utilisateurs.
- De n'effectuer des accès aux contenus marqués comme « privés » qu'en présence de l'utilisateur ou avec son autorisation écrite, à l'exception des cas d'atteinte à la sécurité ou à la disponibilité des informations indispensables de la continuité du service sous couvert d'autorisation du RSSI. Cette obligation ne concerne pas l'utilisation d'outils automatiques qui ne visent pas individuellement l'utilisateur (antivirus, inventaire logiciel, logiciel de sauvegarde…).
- D'être transparent vis-à-vis des utilisateurs sur l'étendue des accès aux informations dont il dispose techniquement de par sa fonction.
- D'informer les utilisateurs et de les sensibiliser aux problèmes de sécurité informatique inhérents au système, de leur faire connaître les règles de sécurité à respecter, aidé par le RSSI.
- De se conformer aux mesures de sécurité de la PSSI de l'ENSAIT.
- De répondre favorablement, et dans les délais les plus courts, à toutes consignes de surveillance, de recueil d'information et d'audit émis par le RSSI.
- De traiter en première priorité toute violation des règles SSI et tout incident de sécurité qu'il est amené à constater, puis d'informer sans délai le RSSI, et d'appliquer sans délai ses directives pour le traitement de l'incident. L'administrateur peut ainsi être conduit à communiquer des informations confidentielles ou soumises au secret des correspondances dont il aurait eu connaissance, si elles mettent en cause le bon fonctionnement des systèmes d'information, ou leur sécurité, ou si elles tombent dans le champ de l'article 40 alinéa 2 du code de procédure pénale[2].

<u>Le Responsable de la Sécurité du Système d'Information a le droit :</u>

- D'accéder à toutes données du système d'information, notamment les journaux informatiques des applications ou des systèmes, lorsque cet accès est rendu nécessaire par le traitement d'un incident de sécurité ou sur demande de la chaîne de sécurité du système d'information.
- De requérir toute l'aide nécessaire des administrateurs dans le déroulement de sa tâche de chargé de sécurité, lorsque cela s'avère indispensable (droit d'accès, éloignement, temps de réaction, technicité…).
- D'interdire temporairement ou définitivement l'accès aux ressources informatiques à un utilisateur qui ne respecte pas la Charte d'utilisation des ressources informatiques annexée au

[1] Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. Loi n°2006-961 du 1 er août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information.

[2] Obligation faite à tout fonctionnaire d'informer sans délai le Procureur de la République de tout crime et délit dont il a connaissance dans l'exercice de ses fonctions

règlement intérieur, ainsi qu'à un administrateur qui ne respecte pas la présente charte. Dans ces cas il doit en informer la direction de l'ENSAIT.

- De saisir l'autorité hiérarchique des manquements graves résultant du non-respect de cette charte.

Le Responsable de la Sécurité du Système d'Information a le devoir :

- De respecter tous les devoirs des administrateurs lorsqu'il a accès au système d'information.
- D'informer tous les acteurs, de diffuser la présente charte par tous moyens appropriés, de veiller à la bonne application de cette charte par tous les acteurs des systèmes d'informations.
- De respecter les dispositions légales et réglementaire concernant le système d'information[3] et pour se faire, de se renseigner, si nécessaire, auprès de sa hiérarchie, du service juridique et du délégué à la protection des données de l'ENSAIT.
- De respecter la confidentialité des informations auxquelles il accède lors de ses tâches, quel qu'en soit le support, en particulier :
  - Les données à caractère personnel contenues dans le système d'information.
  - Les fichiers utilisateurs.
  - Les flux sur les réseaux.
  - Les courriers électroniques.
  - Les mots de passe.
  - Les sorties imprimantes.
  - Les traces des activités des utilisateurs.

[3] Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. Loi n°2006-961 du 1 er août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information.