DDN/RSSI

Engagement éthique et déontologique de l'administrateur systèmes, réseaux et de système d'informations

SOMMAIRE.

Préambule

Le présent engagement éthique et déontologique de l'administrateur systèmes, réseaux et système d'informations de l'Université d'Angers est destiné à préciser les droits et les devoirs de toute personne chargée de la gestion de ressources informatiques, de télécommunication ou logicielles de l'Université d'Angers, il n'a pas pour but de décrire les métiers de l'administrateur systèmes, réseaux et systèmes d'information.

Ces engagements sont promulgués en référence à la Charte d'usage du Système d'Information de l'Université d'Angers.

Acronymes utilisés :

SSI Sécurité du Système d'Information

RSSI Responsable de la Sécurité du Système d'Information

Article I. Définitions

Section I.1 Administrateur

L'administrateur systèmes, réseaux et systèmes d'information est toute personne, employée ou non par l'Université d'Angers, à laquelle est confiée la responsabilité d'un système informatique, d'un réseau, d'équipements de téléphonie, de la maîtrise d'œuvre d'application ou d'un traitement de données, administrés par une entité de l'établissement, ou de plusieurs de ces éléments. Une personne à qui est conférée une telle responsabilité sera désignée dans la suite de ce document 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 quant à l'utilisation et à la gestion des moyens informatiques ou de télécommunication. Dans le cadre de son activité, il pourra être amené à avoir accès aux informations des autres utilisateurs, informations parfois confidentielles.

Section I.2 Correspondant sécurité ou chargé de sécurité

Le correspondant sécurité (parfois nommé chargé de sécurité) du système d'information est la personne relais du responsable de sécurité du système d'information (RSSI) de l'Université d'Angers pour son entité. Suivant la taille de l'entité, un ou plusieurs collaborateurs peuvent lui être adjoints.

De par son rôle dans la chaîne de sécurité du système d'information, il pourra être amené à avoir accès à des informations des autres utilisateurs, informations parfois confidentielles.

Les règles de déontologie définies pour l'administrateur s'entendent également pour le correspondant sécurité.

Section I.3 Responsable fonctionnel de système informatique

Le responsable fonctionnel est la personne en charge administrative de l'entité (directeur de laboratoire, directeur d'UFR, chef de service…), et par extension, assurant la responsabilité fonctionnelle du système informatique de l'entité. En revanche cette responsabilité n'entraîne aucunement la détention de droits d'administrateurs, et généralement, le responsable fonctionnel n'entre pas dans la chaîne de sécurité du système d'information, sauf s'il a le rôle de correspondant SSI de l'entité.

Section I.4 Chaîne de sécurité du système d'informations

Sous la responsabilité du RSSI, elle est composée des correspondants sécurité qui centralisent et relaient les informations provenant des administrateurs lors du traitement d'incidents. Son rôle est également de définir des procédures en lien avec les responsables fonctionnels pour permettre l'accès des utilisateurs au système d'information en respectant les contraintes de disponibilité, de confidentialité et d'intégrité.

Article II. Droits et devoirs spécifiques des administrateurs

Section II.1 Tout administrateur a le droit :

Dans le cadre du respect de la Politique de Sécurité du Système d'Information d'établissement ;

- 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 de réseau (métrologie, surveillance…) ;
- de mettre en place toutes procédures appropriées pour vérifier la bonne application des règles de contrôle d'accès aux systèmes et aux réseaux définies dans la Politique de Sécurité du Système d'Information, 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 - tant que la situation ne l'exige pas - de ne pas les altérer ;
- d'établir des procédures de surveillance de toutes les tâches exécutées sur la machine, afin de déceler les violations ou les tentatives de violation du présent engagement et de la charte d'usage du système d'information, sous l'autorité de son responsable fonctionnel et en relation avec le correspondant sécurité informatique ;
- de prendre des mesures conservatoires si l'urgence l'impose, sans préjuger des sanctions résultant des infractions aux différentes chartes. Mesures telles que restriction de la connectivité, suppression de fichiers (après sauvegarde sur support isolé) qu'il estimerait susceptibles de porter atteinte à l'intégrité, à la disponibilité, à la confidentialité et à la sécurité des systèmes d'information ;
- de ne pas intervenir sur du matériel n'appartenant pas à l'établissement, sauf à l'isoler du système d'information et du réseau de l'établissement en cas de non-respect des consignes.

Section II.2 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, de la chaîne fonctionnelle SSI, ou des services juridiques de l'établissement.
- 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...), 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,

1 Loi Informatique et Liberté, Loi pour la confiance dans l'économie numérique (LCEN), Code des postes et des communications électroniques, Code de la propriété intellectuelle, Loi relative au droit d'auteur et aux droits voisins dans la société de l'information (DADVSI), Loi favorisant la diffusion et la protection de la création sur internet (HADOPI) …

    - 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 sous couvert d'autorisation de la chaîne SSI ou de l'utilisation d'outils automatiques qui ne visent pas individuellement l'utilisateur (antivirus, inventaire logiciel…) ;
- 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 responsable fonctionnel ;
- de garantir la transparence dans l'emploi d'outils de prise en main à distance ou toute autre intervention sur l'environnement de travail individuel de l'utilisateur (notamment en cas d'utilisation du mot de passe de l'utilisateur) : limitation de telles interventions au strict nécessaire avec accord préalable de l'utilisateur ;
- de s'assurer de l'identité et de l'habilitation de l'utilisateur lors de la remise de tout élément du système d'information (information, fichier, compte d'accès, matériel...), en collaboration avec le responsable fonctionnel ;
- de se conformer à la politique de sécurité des systèmes d'information de l'établissement ;
- de répondre favorablement, et dans les délais les plus courts, à toute consigne 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 correspondant de sécurité informatique ou le RSSI selon la procédure prévue par la chaîne fonctionnelle de sécurité, et d'appliquer sans délai les directives du RSSI 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].

2 « Toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs. »

Section II.3 Le Correspondant Sécurité du Système d'Information a le droit :

- 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. (cf Section II.1), lorsque cela s'avère indispensable (droit d'accès, éloignement, temps de réaction, technicité…).

Section II.4 Le Correspondant Sécurité du Système d'Information a le devoir :

- De respecter tous les devoirs des administrateurs lorsqu'il a accès au système d'information. (cf. Section II.2).

Section II.5 Le responsable fonctionnel de système informatique a le droit :

- d'interdire temporairement ou définitivement l'accès aux ressources informatiques à un utilisateur qui ne respecte pas la charte d'usage du système d'informations, ainsi qu'à un administrateur qui ne respecte pas la présente charte ;
- de saisir l'autorité hiérarchique des manquements graves résultant du non respect de cette charte pouvant déclencher des procédures disciplinaires ou judiciaires.

Section II.6 Le responsable fonctionnel de système informatique a le devoir :

- d'informer tous les acteurs, de diffuser le présent engagement par tous moyens appropriés; de veiller à la bonne application de cet engagement par tous les acteurs des systèmes d'informations.

Annexe

Principales références législatives

(A) Infractions prévues par le Nouveau Code pénal

Crimes et délits contre les personnes

Atteintes à la personnalité : (Respect de la vie privée art. 9 du code civil)

- Atteintes à la vie privée (art. 226-1 al. 2 ; 226-2 al. 2, art.432-9 modifié par la loi nº2004-669 du 9 juillet 2004) ; atteintes à la représentation de la personne (art. 226-8)
- Dénonciation calomnieuse (art. 226-10)
- Atteinte au secret professionnel (art. 226-13)
- Atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques (art. 226-16 à 226-24, issus de la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

Atteintes aux mineurs : (art. 227-23 ; 227-24 et 227-28)

- Loi 2004- 575 du 21 juin 2004 (LCEN)

Crimes et délits contre les biens

- Escroquerie (art. 313-1 et suite)
- Atteintes aux systèmes de traitement automatisé de données (art. 323-1 à 323-7 modifiés par la loi nº 2004-575 du 21 juin 2004).

Cryptologie

- Art. 132-79 (inséré par loi nº 2004-575 du 21 juin 2004 art. 37)

(B) Infractions de presse (loi 29 juillet 1881, modifiée)

- Provocation aux crimes et délits (art.23 et 24)
- Apologie des crimes contre l'humanité, apologie et provocation au terrorisme, provocation à la haine raciale, « négationnisme » contestation des crimes contre l'humanité (art. 24 et 24 bis)
- Diffamation et injure (art. 30 à 33)

(C) Infraction au Code de la propriété intellectuelle

- Contrefaçon d'une œuvre de l'esprit (y compris d'un logiciel) (art. 335-2 modifié par la loi nº 2004-204 du 9 mars 2004, art. 34 - et art. 335-3)
- Contrefaçon d'un dessin ou d'un modèle (art. L521-4 modifiée par la loi nº 2004-204 du 9 mars 2004, art. 34)
- Contrefaçon de marque (art. L716-9 - modifié par la loi nº 2004-204 du 9 mars 2004, art.34 -et suivants)

Il est rappelé que cette liste n'est qu'indicative et que la législation est susceptible d'évolution.