Paris, le 9 novembre 2006

Charte de l'administrateur de système et de réseau

Table des matières

1 Préambule

La présente Charte de l'Administrateur de Système et de Réseau de l'INSERM est destinée à déterminer les devoirs, les pouvoirs et les droits des ingénieurs et des techniciens qui administrent la sécurité des réseaux, des ordinateurs et du système d'information de l'INSERM.

Cette Charte est promulguée en référence à la Charte de l'utilisateur des ressources informatiques et des services Internet de l'INSERM, qu'elle complète et dont elle est inséparable.

2 Définitions

Les *entités* de l'INSERM, ses *ressources informatiques*, ses *services Internet* et les *utilisateurs* du Système d'Information qu'ils constituent sont définies ici comme dans la Charte de l'utilisateur des ressources informatiques et des services Internet de l'INSERM.

L'*administrateur* d'un système ou d'un réseau de l'INSERM est toute personne, employée ou non par l'INSERM, à laquelle a été confiée explicitement et par écrit, sous la forme d'une lettre de mission, d'un profil de poste annexé au contrat de travail ou d'un contrat de prestations de service, la responsabilité d'un système informatique, d'un réseau ou d'un sous-réseau administrés par une entité

de l'INSERM, ou de plusieurs de ces éléments. Une personne à qui a été 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.

Le *comité de coordination* de sécurité du système d'information (SSI) est constitué de responsables chargés d'apprécier la sistuation de la sécurité des systèmes d'information de l'Inserm, d'émettre des propositions et des recommandations dans le domaine SSI, d'évaluer l'impact des mesures mises en œuvre, et de proposer les activités de formation, d'information et de sensibilisation de nature à améliorer les conditions de leur application. Les membres de ce comité de coordination sont notamment le Directeur Général de l'Inserm, le Responsable de Sécurité des Systèmes d'Information (RSSI) de l'INSERM, le Responsable de la Sécurité Opérationnelle au sein du Département du Système d'Information (DSI) de l'INSERM, le Correspondant Informatique et Libertés de l'INSERM et d'autres personnes désignées par le Directeur Général de l'INSERM.

Les devoirs, les pouvoirs et les droits de l'administrateur, définis dans la présente Charte, constituent ensemble les *responsabilités SSI* de l'administrateur.

Les consignes du comité de coordination SSI s'imposent aux administrateurs de systèmes et de réseaux pour l'exercice de leurs responsabilités SSI dans leur périmètre d'activité.

3 Responsabilités du comité de coordination SSI

3.1 Surveillance et audit

Le comité de coordination SSI organise la surveillance et l'audit de toutes les activités des systèmes et de tous les trafics réseau sur les infrastructures administrées par l'INSERM.

Pour ce faire, le comité de coordination SSI est habilité à donner des consignes de surveillance, de recueil d'information et d'audit aux administrateurs concernés.

3.2 Contrôle d'accès

Le comité de coordination SSI définit des règles de contrôle d'accès aux systèmes et aux réseaux conformes à la présente Charte et à la Charte de l'utilisateur des ressources informatiques et des services Internet de l'INSERM.

3.3 Vérification

Le comité de coordination SSI et les administrateurs concernés sont habilités à entreprendre toutes actions appropriées pour vérifier la bonne application des règles de contrôle d'accès aux systèmes et aux réseaux définies à l'article précédent, ainsi que pour détecter leurs vulnérabilités.

4 Responsabilités de l'administrateur de système et de réseau

4.1 Enregistrement des incidents de sécurité

L'administrateur conserve une trace écrite des incidents de sécurité survenus dans son périmètre d'activité. Cette trace doit comporter les indications de date et d'heure des événements considérés, et une description de ces événements.

4.2 Notification des incidents de sécurité

Les administrateurs de système et de réseau sont tenus de déclarer tout incident de sécurité au RSSI et au responsable de le sécurité opérationnelle. Les directives du RSSI et du responsable de la sécurité opérationnelle pour des actions relatives aux incidents sont mises en application sans délais.

4.3 Journalisation et archivage

L'administrateur active sur les systèmes dont il a la responsabilité les journaux nécessaires à l'identification et à la reconstitution des séquences d'événements qui pourraient constituer un incident de sécurité, ou qui pourraient faire l'objet d'une commission rogatoire émise par les autorités judiciaires. Il archive les données ainsi recueillies dans des conditions propres à en assurer l'intégrité, la disponibilité, l'authenticité et la confidentialité.

Il mène cette activité de journalisation et d'archivage dans des conditions qui garantissent le respect des lois et des règlements relatifs aux libertés publiques et privées, au secret des correspondances, au droit d'accès à l'information, et il veille notamment à détruire tous les journaux qui comportent des données nominatives à l'expiration d'un délai qui ne peut excéder un an, ou le délai légal à la date considérée.

Parmi les textes législatifs et réglementaires qui s'appliquent à cette activité, il convient d'accorder une attention particulière à la Norme simplifiée n°46 de la Commission Nationale Informatique et Libertés, « destinée à simplifier l'obligation de déclaration des traitements mis en œuvre par les organismes publics et privés pour la gestion de leurs personnels ».

4.4 Examen des journaux

L'administrateur examine régulièrement les journaux mentionnés à l'article ci-dessus.

4.5 Dérogations aux règles SSI

Les règles SSI mentionnées dans la présente Charte, dans la Charte de l'utilisateur des ressources informatiques et des services Internet de l'INSERM, ou édictées par le RSSI de l'INSERM, par le Responsable de la Sécutité Opérationnelle au sein du DSI de l'INSERM ou par le comité de coordination SSI s'imposent à tous les utilisateurs des Systèmes d'Information de l'INSERM, qu'ils soient on non des employés de l'INSERM. Les administrateurs de systèmes et de réseaux de l'INSERM ont pour mission de les mettre en œuvre et de les faire respecter dans leur périmètre d'activité.

4.6 Identification des utilisateurs et contrôles d'accès

Dans leur périmètre d'activité, les administrateurs responsables sont seuls habilités à mettre en place et à administrer les systèmes d'identification et d'authentification des utilisateurs conformes aux directives du comité de coordination SSI. Il en va de même pour les dispositifs de contrôle d'accès aux systèmes, aux réseaux et aux données.

Sauf exception formulée par un document écrit signé d'un responsable d'entité, seuls l'administrateur local et ses collaborateurs immédiats possèdent les droits d'administrateur sur les postes de travail des utilisateurs des SI de l'INSERM.

4.7 Audits périodiques

Les administrateurs procèdent deux fois par an à un audit des comptes des utilisateurs et des droits d'accès associés, pour vérifier leur validité et leur exactitude.

5 Mise en œuvre et litiges

5.1 Rapport des violations des règles SSI

Pour toute violation des règles SSI qu'il est amené à constater, l'administrateur établit un rapport écrit destiné au comité de coordination SSI et à ses responsables hiérarchiques.

5.2 Veille SSI

Les administrateurs exercent régulièrement une activité de veille scientifique et technologique dans le domaine SSI. Ils sont abonnés aux listes de diffusion qui publient les découvertes de vulnérabilités. Ils participent notamment aux activités de formation, d'information et de sensibilisation entreprises par le comité de coordination SSI.

5.3 Attitude à l'égard des violations de la loi

Lorsque l'administrateur constate des violations de la loi dans son périmètre d'activité, il en fait rapport au comité de coordination SSI et à ses responsables hiérarchiques, qui prendront les mesures adéquates.

5.4 Attitude à l'égard des violations des règles SSI

La direction de l'INSERM, ou son représentant qualifié, peut révoquer le compte et les droits d'accès au réseau et aux données d'un utilisateur qui aurait violé les règles SSI mentionnées dans la Charte de l'utilisateur des ressources informatiques et des services Internet de l'INSERM.