



**ACADÉMIE
DE CRÉTEIL**

*Liberté
Égalité
Fraternité*

Politique de Sécurité des Systèmes d'Information de l'Académie de Créteil

ANNEXE 4

Charte des administrateurs informatiques de
l'académie de Créteil

Sommaire

I. Contexte.....	4
II. Objet.....	4
III. Définitions.....	5
IV. Identification des administrateurs informatiques.....	6
V. Les droits de l'administrateur informatique.....	7
VI. Les obligations de l'administrateur informatique.....	8
VII. Respect de la législation et de la présente charte.....	10
VIII. Engagements.....	11
Engagement personnel de l'administrateur informatique.....	11
Engagement du supérieur hiérarchique.....	11

I. Contexte

L'information et les systèmes d'information associés constituent des éléments indispensables pour la conduite des activités et missions de l'académie.

Dans ce contexte, la bonne administration des données et des ressources les supportant, les transportant ou les traitant, participe directement à la performance et à la bonne réalisation de ces missions et activités.

Les personnels en charge de cette administration, appelés généralement « administrateurs systèmes, réseaux et systèmes d'information », 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 par ailleurs un caractère confidentiel. Ils effectuent également régulièrement des actions potentiellement sensibles : changement de mécanismes de protection, création ou modification de comptes utilisateurs et des droits associés, suppression de fichiers, transfert de données, etc.

Toute action de ce type, mal exécutée, peut entraîner de graves conséquences telles que l'indisponibilité de certaines applications et l'altération voire la destruction ou la compromission d'informations essentielles.

En raison de leurs prérogatives, ces personnels ont un rôle essentiel, requérant discrétion et diplomatie : leur démarche se doit d'être impartiale. Leurs interventions ne doivent pas outrepasser 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 est destinée à préciser les principes structurant leurs obligations et leurs droits dans le cadre d'actions qu'ils sont amenés à effectuer. Elle s'inscrit en cohérence et en complément de la charte académique régissant l'usage des technologies de l'information et de communication par les personnels de l'Éducation nationale ainsi que des chartes des établissements et des écoles.

II. Objet

Les administrateurs informatiques, comme tous les agents de l'académie de Créteil, s'engagent à respecter les obligations précisées dans la charte régissant l'usage des technologies de l'information et de la communication par les personnels de l'académie de Créteil.

La présente charte a pour objet de préciser les droits et obligations des administrateurs informatiques dans l'exercice de leur fonction.

Elle s'applique à tout administrateur informatique amené à intervenir sur le système d'information de l'académie de Créteil, qu'il soit fonctionnaire, contractuel¹, stagiaire², vacataire ou encore prestataire.

¹ Le respect de la présente charte figurera dans le contrat.

² Le respect de la présente charte figurera dans la convention de stage s'il y a lieu.

Elle concerne également toute personne appelée à valider les demandes d'ouverture de droits et d'autorisations appropriés des administrateurs informatiques ainsi que les supérieurs hiérarchiques de ces administrateurs.

Elle se doit, par ailleurs, d'être connue de toute personne impliquée dans la gestion des ressources humaines d'administrateurs informatiques ou la passation de contrats avec des sociétés extérieures.

Plus particulièrement, elle s'applique aux administrateurs des espaces numériques de travail déployés dans les établissements et les écoles de l'académie, qu'ils soient agents ou personnels d'un prestataire privé.

III. Définitions

Système d'information:

Ensemble des ressources matérielles, logicielles, applications, bases de données et réseaux de télécommunications, pouvant être mis à disposition par l'institution et permettant de collecter, regrouper, classifier, stocker, traiter et diffuser de l'information.

L'informatique nomade tels que les assistants personnels, les ordinateurs portables, les téléphones portables... est également un des éléments constitutifs du système d'information.

Ressource:

Élément informationnel³ ou matériel

Ressource non institutionnelle⁴:

Ressource mise à disposition des utilisateurs par des tiers.

Institution:

Tout service (administration centrale, rectorat, inspection académique) ou établissement d'enseignement relevant de l'Éducation Nationale.

Administrateur informatique:

Le terme « administrateur Informatique » désigne toute personne ayant un droit d'administration sur une ressource du Système d'Information (SI) de l'académie dont il a pour mission d'assurer le bon fonctionnement, la sécurité ou encore l'assistance aux utilisateurs de celles-ci.

L'administrateur informatique intervient uniquement sur les ressources placées sous sa responsabilité : selon le cas, il procède à des opérations de configuration, de tests, de supervision, de contrôle, de maintenance, de sauvegarde et d'archivage ou encore de gestion des évolutions. Il peut également être en charge d'actions d'assistance et, de manière générale, participe activement à la mise en place de la politique de sécurité académique (ou plus particulièrement de celle de son établissement ou de l'entité à laquelle il est rattaché).

3 Pour exemple, une ressource informationnelle peut être un fichier informatique, un document rédigé, etc.

4 Les ressources matérielles personnelles ou les services en ligne proposés par des tiers font parties des ressources non institutionnelles.

L'administrateur informatique peut ainsi être un administrateur système ou réseau de la direction des systèmes d'information de l'académie, un conseiller de la plateforme d'assistance informatique académique, une personne ressource dans un établissement public ou une circonscription du premier degré, un administrateur d'espace numérique de travail, un prestataire privé, un administrateur réseau dans une commune, etc.

Les utilisateurs qui disposent uniquement de droits « administrateur » sur leur poste de travail ne sont pas considérés à ce titre comme « administrateur informatique » au sens de la présente charte.

IV. Identification des administrateurs informatiques

Les responsables des services académiques (rectorat, DSDEN, circonscriptions, etc.) doivent identifier dans leur structure les personnels exerçant des missions d'administrateur informatique afin de leur faire signer la présente charte.

Il en est de même au sein de chaque établissement pour le chef ou directeur d'établissement et adjoint(s).

La fiche de poste ou la lettre de mission spécifiera le périmètre d'action et les ressources impliquées:

- s'agissant des personnels de prestataires extérieurs privés, ces éléments seront précisés dans le contrat,
- s'agissant des personnels relevant de l'Education Nationale en charge de missions nationales, ces éléments seront consignés dans une fiche descriptive transmise aux responsables concernés,
- s'agissant des personnels relevant des collectivités, ces éléments seront précisés dans des conventions de partenariat.

Le responsable de la sécurité des systèmes d'information de l'académie (RSSI) ou son adjoint, doivent être informés de l'identité des administrateurs informatiques; ils peuvent être amenés à consulter leur lettre de mission, fiche de poste, fiche descriptive ou éléments significatifs du contrat afin de vérifier la pertinence et le bon usage des accès privilégiés attribués.

Chaque responsable concerné se doit de tenir à jour la liste des administrateurs informatiques placés sous sa responsabilité ainsi que le périmètre de leur champ d'intervention.

V. Les droits de l'administrateur informatique

En application des consignes qui lui ont été transmises, l'administrateur informatique peut prendre toute disposition nécessaire afin d'assurer le bon fonctionnement et la sécurité des composants des systèmes d'Information dans son périmètre de responsabilité tels que désignés dans sa fiche de poste.

En particulier, il peut:

- isoler, suspendre ou reconfigurer des comptes utilisateurs, équipements ou applications informatiques pouvant compromettre la sécurité du système d'information. Lorsque la situation l'exige⁵ il demande l'autorisation de son supérieur hiérarchique et du Responsable de la Sécurité des Systèmes d'Information.
- procéder à des vérifications techniques sur les fichiers et bases de données, la messagerie, les connexions à Internet, les fichiers de journalisation, etc., afin de déceler toute anomalie ou incident de sécurité qui pourrait porter atteinte au bon fonctionnement et à la sécurité des systèmes d'information dans les activités d'administration et d'assistance,
- traiter (détection, analyse, éradication, filtrage, etc.) ou s'assurer du traitement de tout flux informatique présentant des risques de sécurité (par exemple: virus, intrusion, utilisation d'un logiciel interdit ou potentiellement dangereux, etc. Si nécessaire, il sera demandé à l'administrateur de faire remonter à son responsable et au RSSI, des informations relatives à la sécurité, sous forme de statistiques régulières ou de signalisation ponctuelle. Sur la base de ces données statistiques, l'administrateur peut les alerter relativement à toute utilisation de ressources informatiques qui apparaîtrait comme non conforme à la charte régissant les usages des systèmes d'information et du numérique par les personnels de l'académie.

Les limites de l'intervention de l'administrateur informatique sont fixées par la réglementation en vigueur, par la présente charte et par la fiche de poste ou tout autre document qui définit ses missions.

Il ne peut être contraint à enfreindre la loi: ainsi, il doit refuser de faire un contrôle ou une action qui ne respectent pas les obligations légales ou les droits élémentaires des utilisateurs comme, par exemple, l'envoi d'un fichier contenant des données confidentielles, envoi dûment autorisé par les responsables concernés et effectué dans un cadre légal mais n'utilisant pas des moyens sécurisés.

Les administrateurs seront informés sur la législation en vigueur et les implications légales de leurs missions.

⁵ Par exemple, dans le cas où il s'agit de couper l'accès à un site attaqué pour préserver l'accès aux autres ressources

VI. Les obligations de l'administrateur informatique

L'administrateur informatique est soumis à une obligation de confidentialité et de non divulgation liée à ses activités.

C'est pourquoi:

- les permissions d'administration attribuées à un administrateur ne sont utilisées que pour mener à bien les tâches qui lui sont confiées,
- l'administrateur prend connaissance des informations contenues dans les systèmes d'information ou donne accès à celles-ci seulement dans le cadre de ses fonctions et/ou sur demande explicite de son responsable ou en son absence du RSSI. Un résumé succinct de l'action devra être consigné,
- le devoir de réserve et le principe de neutralité lui imposent l'interdiction absolue de faire de sa fonction l'instrument d'une propagande quelconque,
- les outils mis à sa disposition ne sont utilisés que dans un but professionnel d'administration, supervision, exploitation, maintenance ou d'assistance,
- les seuls cas dans lesquels il autorise un accès aux données personnelles des utilisateurs sont les cas particuliers prévus par la loi, sur demande explicite de l'utilisateur à des fins d'assistance ou lorsque des personnes ont été dûment habilitées et préalablement désignées,
- il s'engage à ne pas faire état ni utiliser les informations qu'il peut être amené à connaître dans le cadre de ses fonctions,
- en cas d'assistance, il ne prend en main, à distance ou non, le poste de travail d'un utilisateur qu'avec l'autorisation explicite de ce dernier et ne se connecte qu'aux seules ressources nécessaires à l'accomplissement de sa mission d'assistance,
- il a le devoir de ne pas abuser de ses prérogatives: les contrôles réalisés doivent être faits non seulement en toute transparence mais aussi de manière proportionnelle et adaptée à la finalité présentée à l'utilisateur lors de l'information préalable à ces contrôles,
- il s'efforce d'éviter tout conflit pouvant exister entre ses intérêts personnels et ceux du service. Il informe sa hiérarchie de tout conflit d'intérêt dans lequel il pourrait être impliqué pouvant altérer l'efficacité de sa mission,
- il veille à ce que les logiciels soient utilisés dans les conditions de licences souscrites.

Par ailleurs:

- il documente ses actions et interventions de telle sorte que ses collaborateurs ne soient pas dans un état de dépendance en cas d'absence ou lorsqu'il quitte sa fonction,
- il collabore et coopère avec le RSSI,
- il est tenu de suivre les procédures préalablement définies.

De plus, l'administrateur informatique observe strictement les règles de sécurité et les limites fixées à ses interventions:

- il limite ses actions aux ressources informatiques dont il a la charge et dans le respect de la finalité de sa mission,
- il ne modifie les configurations et les droits d'accès que dans les cas préalablement définis,
- il ne prend pas ses consignes d'une personne non habilitée et fait remonter auprès de son supérieur direct tel que mentionné dans sa fiche de poste et au RSSI toute requête lui paraissant inappropriée ou contraire à la réglementation. En cas de requête qui lui semblerait non appropriée présentée par sa hiérarchie, il a le devoir d'expliquer à celle-ci les raisons de son opposition.
Si cette requête était maintenue, il prévient le RSSI ou en son absence le Secrétaire Général de l'académie.
- il observe les procédures de sécurité établies et il veille, selon les possibilités du système administré, à ce que les mécanismes de traçabilité soient actifs et à ce qu'il n'y ait aucune atteinte à l'intégrité des fichiers de journalisation,
- dans le cadre de la conduite de sa mission et vis-à-vis des ressources à sa charge (serveurs, bases de données, postes de travail utilisateurs, etc.), il utilise les logiciels faisant partie des standards approuvés par l'académie.
Toute installation de logiciel ne faisant pas partie de ces standards doit faire l'objet d'une autorisation préalable et explicite du responsable hiérarchique ou de la Direction des Systèmes d'Information (DSI) de l'académie ou du RSSI.

En cas d'incident de sécurité ou de détection de vulnérabilité:

- il informe son supérieur direct et le RSSI de toute faille ou incident de sécurité qu'il pourrait découvrir ou dont il pourrait avoir connaissance.
- il utilise la chaîne d'alerte quand elle existe,
- il coopère avec le RSSI en cas d'attaque impliquant un composant du système qu'il administre,
- il préserve, conserve et sauvegarde les traces nécessaires à la résolution d'un incident et à toute investigation ultérieure.

Enfin, l'administrateur informatique s'assure de la protection des droits d'accès liés à sa fonction:

- il observe les règles de sécurité en vigueur visant à protéger l'utilisation des comptes et des droits privilégiés qui lui ont été attribués,
- il veille à la protection des postes de travail à partir desquels il exerce ses fonctions et à la gestion des identifiants et mots de passe des comptes privilégiés.

En particulier, les mots de passe utilisés pour les opérations d'administration doivent être robustes et changés régulièrement conformément à la politique de sécurité des mots de passe académique.

Il est rappelé que les droits confiés à un administrateur (et par conséquent les couples identifiant/mot de passe associés) sont confidentiels et donc inaccessibles,

- il n'utilise ses comptes privilégiés que pour les activités et besoins directement liés aux tâches d'administration, d'exploitation ou d'assistance dont il a la charge, étant donné que toute action sur les systèmes d'Information peut faire l'objet d'une journalisation permettant leur imputabilité.

Des contrôles des traces de connexion ou des sessions des administrateurs informatiques peuvent être effectués par le RSSI ou une personne désignée par lui en cas d'incident ou à titre préventif.

Au sein de la direction des systèmes d'information de l'académie, pour les seuls besoins de continuité du service, les administrateurs peuvent également être amenés à consulter les sessions précédentes.

Les administrateurs informatiques en contact avec les utilisateurs, tels les personnels en charge de l'assistance, doivent participer à la sensibilisation de ces derniers:

- en rappelant les principes de la charte académique régissant les usages des systèmes d'information et du numérique et autres chartes en vigueur à tout utilisateur semblant les méconnaître,
- en prévenant les utilisateurs des consignes techniques de sécurité à mettre en œuvre afin de préserver le système d'information et les données professionnelles et privées,
- en participant à l'information des utilisateurs sur les risques qu'ils encourent ou qu'ils font encourir à l'institution du fait de leur comportement (installation de logiciels sans licence acquise officiellement ou potentiellement dangereux, copies de sauvegarde sans autorisation, usage illégal ou non conforme des ressources informatiques, tentative de mise hors circuit d'un dispositif de sécurité, usurpation d'identité, etc.).

Avant toute intervention sur son poste de travail, chaque fois que cela est possible, les administrateurs invitent l'utilisateur à séparer ses documents personnels/privés de ses documents professionnels et à les mettre dans un répertoire portant la mention «personnel» ou «privé» afin de respecter l'intimité de sa vie privée.

VII. Respect de la législation et de la présente charte

L'administrateur informatique s'engage à respecter en toute circonstance la législation en vigueur, notamment celle du Code de l'Education Nationale, ainsi que les règles de la présente charte et celles de la charte régissant les usages des systèmes d'information et du numérique par les personnels de l'académie de Créteil.

VIII. Engagements

Engagement personnel de l'administrateur informatique

Je soussigné,

dans ma fonction d'administrateur informatique, déclare avoir pris connaissance de la **Charte des administrateurs informatiques de l'académie de Créteil** et m'engage à la respecter.

Fait en deux exemplaires à le

Engagement du supérieur hiérarchique

Je soussigné,

Responsable de la structure (RNE, division, service).....

agissant en tant que supérieur hiérarchique de

déclare avoir pris connaissance de la **Charte des administrateurs informatiques de l'académie de Créteil** et m'engage à en respecter les limites définies.

Fait en deux exemplaires à le

L'administrateur informatique et le supérieur hiérarchique conserveront un exemplaire.

La présente charte signée devra être numérisée et retournée au RSSI rsi@ac-creteil.fr