ACADÉMIE
DE VERSAILLES
Liberté
Égalité
Fraternité

L'ACADÉMIE
vous accompagne

POLITIQUE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION DE L'ACADÉMIE DE VERSAILLES

ANNEXE 5

CHARTE DES ADMINISTRATEURS INFORMATIQUES DE L'ACADÉMIE DE VERSAILLES

Sommaire

1. Préambule

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 informatiques », 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 la destruction voire l'altération 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'Education nationale ainsi que des chartes des établissements et des écoles.

2. Définitions

Par *institution*, s'entend tout service académique[1] ou établissement d'enseignement relevant de l'Education nationale dans l'académie de Versailles.

Par *système d'information*[2], s'entend l'ensemble des ressources matérielles, logicielles, applications, bases de données et réseaux de télécommunication pouvant être mises à disposition ou gérées par l'institution dans l'académie de Versailles.

Ces ressources peuvent être notamment :

- des serveurs (d'authentification, de stockage, d'impression, …),
- des éléments d'infrastructure réseau et services internet,
- des équipements de sécurité,

1 Service au sens étendu du terme : ce peut être un service administratif, la délégation académique pour le numérique éducatif (DANE), etc.

2 Il est parfois question de plusieurs systèmes d'information au sein de l'académie lorsque l'on veut distinguer différentes composantes de ce système ou se référer aux seules ressources d'un service spécifique ou d'un établissement.

- des applications, logiciels,
- des bases de données,
- des postes de travail utilisateurs,
- des imprimantes,
- des copieurs,
- des numériseurs,
- des tablettes et ordi phones,
- des équipements téléphoniques (autocommutateur, portable professionnel,…).

Il est à noter que certaines ressources peuvent être des outils mis en œuvre au niveau national par le ministère de l'Education nationale mais gérés ou administrés, pour les utilisateurs ou personnes concernés par des administrateurs de l'académie.

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).

L'administrateur informatique peut ainsi être un administrateur 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 ou 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.

3. Objet

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 Versailles, qu'il soit fonctionnaire, contractuel[3], stagiaire[4], vacataire ou encore prestataire.

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.

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

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

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.

4. Identification des administrateurs informatiques

Au sein de chaque service académique concerné (direction des systèmes d'information, DANE, direction des services départementaux de l'Education nationale, circonscriptions du premier degré, ...), les responsables doivent être informés de l'identité des personnes auxquelles sont attribuées des fonctions d'administrateur informatique.

Il en est de même au sein de chaque établissement pour le chef ou directeur d'établissement et son adjoint[5].

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.

À leur demande, le responsable de la sécurité des systèmes d'information de l'académie (RSSI) et son adjoint[6] 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.

5. 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.

5 Ses adjoints s'il y a lieu.

6 Ou une personne désignée par le RSSI

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'exige[7] il demande l'autorisation de son supérieur hiérarchique et du Responsable de la Sécurité des Systèmes d'Information[8];
- 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 RSSI8, 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 TIC académique[9].

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.

6. 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 RSSI9 (un résumé succinct de l'action sera consigné) ;

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

8 Ou le RSSI adjoint ou une personne désignée par le RSSI.

9 Charte régissant l'usage des technologies de l'information et de communication par les personnels de l'académie de Versailles.

- 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 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, 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'intérêts 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[7] ; 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 ; par ailleurs, 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[7] 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.

En cas d'incident de sécurité :

- il informe son supérieur direct et le RSSI[7] 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[7] 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 notamment 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 incessibles ;
- 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 des collègues de leur équipe.

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 TIC académique 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, ….).

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.

7. 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 TIC académique.

8. Statut de la charte

Le comité technique académique a examiné les dispositions de cette charte lors de sa séance du 27 mai 2014. Sa date d'entrée en vigueur est fixée au 27 mai 2014.

Cette charte sera librement consultable par les personnels de l'académie de Versailles.

Chaque administrateur informatique sera tenu d'en prendre connaissance et de s'engager à la respecter. L'engagement sera signé en deux exemplaires (l'un conservé au sein du service ou établissement et l'autre par l'administrateur lui-même).

Le supérieur direct[10] de l'administrateur concerné s'engage à respecter les limites définies dans la charte : l'engagement sera signé en deux exemplaires (l'un conservé au sein du service ou établissement, l'autre par lui-même).

10 Excepté si l'administrateur informatique est un chef d'établissement.

Annexe 1 : 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 Versailles » et m'engage à la respecter.

Fait en deux exemplaires à …….. le ……..

Annexe 2 : engagement du supérieur direct

Je soussigné, ……. agissant en tant que supérieur direct de ……. déclare avoir pris connaissance de la « Charte des administrateurs informatiques de l'académie de Versailles » et m'engage à en respecter les limites définies.

Fait en deux exemplaires à …….. le ……..