Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

académie
Aix-Marseille

RÉGION ACADÉMIQUE
PROVENCE-ALPES-CÔTE D'AZUR

MINISTÈRE
DE L'ÉDUCATION NATIONALE
MINISTÈRE
DE L'ENSEIGNEMENT SUPÉRIEUR,
DE LA RECHERCHE
ET DE L'INNOVATION

CHARTE DES ADMINISTRATEURS DU SYSTÈME D'INFORMATION DE L'ACADÉMIE D'AIX-MARSEILLE

1 PRÉAMBULE

Par *institution*, il faut entendre tout service académique, école, ou établissement d'enseignement secondaire de l'académie d'Aix-Marseille.

Le *système d'information* recouvre l'ensemble des ressources matérielles, logicielles, applications, bases de données et réseaux de télécommunications, pouvant être mis à disposition par l'institution ou par les collectivités au service de celle-ci. Il est aussi constitué des dispositifs numériques nomades personnels connectés à l'institution.

Le mot *propriétaire* se comprend en termes de responsabilités, et non au sens de propriété juridique. Les directeurs ainsi que leurs chefs de service sont propriétaires de leurs données métier.

Le terme d'*administrateur* recouvre tout personnel ayant des droits d'accès étendus au système d'information à des fins d'administration, maintenance ou assistance sur les données et/ou des ressources les supportant, les transportant ou les traitant, dans le cadre de son activité professionnelle et quel que soit son statut. Il s'agit notamment de :

- tout agent titulaire ou non titulaire de l'institution ou d'une collectivité concourant au travers de ces tâches d'administration à l'exécution des missions du service public de l'éducation,
- tout consultant ou prestataire ayant contracté avec l'institution ou avec une collectivité territoriale ayant compétence partagée avec l'État en matière d'éducation.

2 OBJECTIFS DE LA CHARTE

Les droits étendus dont les administrateurs disposent pour les besoins de leur mission, leur ouvrent l'accès à un grand nombre d'informations pouvant être sensibles, confidentielles ou d'ordre privé.

Les administrateurs peuvent effectuer des actions sensibles : changement de mécanismes de protection, création ou modification de comptes utilisateurs et des droits associés, suppression de fichiers, transfert de données, etc. Les actions de ce type sont susceptibles d'avoir pour conséquences l'indisponibilité de certaines applications et l'altération, voire la destruction ou la compromission, d'informations essentielles.

Enfin, ils sont souvent les premiers témoins de situations ou d'incidents pouvant déboucher sur des mesures disciplinaires ou des poursuites judiciaires.

En raison de leurs prérogatives, ces personnels ont un rôle essentiel, requérant discrétion et diplomatie : leur démarche se doit d'être exemplaire et impartiale. Conformément aux obligations statutaires propres à tout agent public, et notamment celles liées aux devoirs de réserve, loyauté, probité, secret et discrétion professionnels, leurs interventions ne doivent pas outrepasser leurs attributions ni relever d'actions effectuées pour leur propre compte ou par intérêt personnel. Ils doivent également être protégés des pressions qui pourraient s'exercer à leur encontre afin d'exploiter les accès dont ils bénéficient.

Le bon fonctionnement du système d'information et la confiance des usagers dans ce dernier suppose le respect des dispositions législatives et réglementaires, notamment le

respect des règles visant à assurer la sécurité, la performance des traitements et la conservation des données.

La présente charte précise le cadre légal, réglementaire et déontologique dans lequel doivent s'inscrire les actions d'administration des systèmes d'information. Elle s'inscrit en complément de la **charte régissant l'usage du système d'information par les personnels de l'académie d'Aix-Marseille** publiée au BA spécial n°288 du 14 avril 2014 relatif aux chartes numériques.

La charte s'appuie sur une annexe juridique qui rappelle les dispositions législatives et réglementaires en vigueur pour son application. Elle peut être complétée par des guides définissant les principales règles et pratiques d'usage.

3 ADMINISTRATEUR D'UN SYSTÈME D'INFORMATION

3.1 Identification des administrateurs d'un système d'information

Les propriétaires de l'information tiennent à jour, sur le périmètre de leur responsabilité, la liste des profils d'accès en administration et des services qui leurs sont associés, en précisant la nature et le périmètre du champ d'intervention.

Les responsables de chaque entité ou service de l'institution tiennent à jour, pour les profils d'accès d'administration ouvert dans leur service, la liste des administrateurs placés sous leur responsabilité qui sont associés à ces profils.

Lorsqu'il s'agit de personnels de prestataires extérieurs, ces éléments sont précisés dans le contrat.

Les listes des profils d'accès et des identités des différents administrateurs sont communiquées, à sa demande, au responsable de la sécurité des systèmes d'information (RSSI) de l'institution concernée.

3.2 Attendus de la fonction

3.2.1 Compétence

L'institution s'assure que l'administrateur dispose des compétences requises par la fonction dans les domaines :

- techniques relatifs aux ressources matérielles et logicielles gérées ;
- des lois et règlements applicables au système d'information administré, leurs évolutions et, plus généralement, le domaine juridique des nouvelles technologies ;
- de la politique de sécurité des systèmes d'information de l'institution ;
- de l'application à ces systèmes des mesures de sécurité et des mesures d'urgence ;
- du suivi des vulnérabilités du (des) système(s) servi(s), des menaces pesant sur eux et des méthodes d'attaques de ces systèmes ;
- du suivi du niveau d'alerte SSI et de l'actualité de la menace.

Elle évalue les besoins en formation de l'administrateur et veille au maintien de ses compétences.

L'administrateur met en œuvre la politique de sécurité de l'information de l'institution. Il déploie les mesures qui s'imposent sur son périmètre. Il informe le RSSI de tout incident de sécurité dès sa constatation.

3.2.2 Principe de maîtrise des droits d'administration

Lorsque cela est possible, l'institution met en place des plateformes de gestion des accès à privilèges afin d'assurer la traçabilité et l'imputabilité des actes d'administration. À défaut, elle privilégie les comptes d'accès individuels pourvus des privilèges d'administration. Les comptes d'accès génériques tels que ***root*** ou ***administrateur*** ne sont utilisés qu'en dernier recours, les authentifications par clés individuelles doivent alors être privilégiées.

Lorsque l'authentification est réalisée au moyen d'un mot de passe celui-ci doit être suffisamment long et complexe. Il doit être changé régulièrement selon un rythme propre à ne pas gêner l'administration, conformément aux préconisations de la politique de sécurité.

L'administrateur ne peut faire usage de ses droits à d'autres fins que celles de sa mission et sur le périmètre qui lui est dévolu. Il s'interdit tout accès à toute information hors du champ de sa mission d'administration. Il ne modifie les configurations et les droits d'accès que dans le respect de procédures d'administration ou d'exploitation définies.

Pour toute autre tâche que celle d'administration et plus généralement lorsque l'utilisation de droits particuliers n'est pas nécessaire, l'administrateur s'identifie sur le système d'information avec un profil n'en comportant pas.

Afin d'assurer la sécurité des opérations d'administration, l'administrateur veille au bon niveau de sécurité du poste à partir duquel ces opérations sont effectuées. Il s'assure notamment de ne pas être administrateur de son poste lors de ces opérations.

3.2.3 Principe de moindre gêne

Les opérations d'administration doivent être conduites de manière à maintenir la continuité du service rendu aux utilisateurs.

L'administrateur effectue ces opérations dans le respect des procédures de planification ou d'exploitation définies. Il recueille l'autorisation de sa hiérarchie et s'assure de l'application de la procédure d'information des utilisateurs et services.

Dans tous les cas, si l'administrateur doit interrompre tout ou partie du service rendu aux utilisateurs, il choisit des plages horaires minimisant la gêne occasionnée et réduit autant que possible la durée et la fréquence des interruptions en accord avec sa hiérarchie.

3.2.4 Secret professionnel

Les administrateurs, en tant que dépositaires de renseignements concernant ou intéressant des particuliers, sont tenus au secret professionnel dans le cadre des règles instituées par le Code pénal.

L'obligation n'est cependant pas absolue. La révélation des secrets acquis est requise ou permise lorsque les nécessités du service ou des obligations légales l'imposent et notamment :

- pour prouver son innocence ;
- lorsque la personne intéressée a donné son autorisation.

Elle est obligatoire notamment dans les cas suivants :

- dénonciation de crimes ou délits dont un fonctionnaire a connaissance dans l'exercice de ses fonctions ;
- communication de renseignements, pièces et documents aux autorités de justice agissant en matière criminelle ou correctionnelle ;
- témoignage en justice en matière criminelle ou correctionnelle ;
- communication des pièces et documents nécessaires au juge administratif saisi d'un recours contre un acte administratif ou au juge judiciaire saisi d'un litige.

3.2.5 Discrétion professionnelle

Comme tout fonctionnaire ou assimilé, l'administrateur doit faire preuve de discrétion professionnelle pour tous les faits, informations ou documents dont il a connaissance dans l'exercice ou à l'occasion de l'exercice de sa fonction. Cette obligation est instituée, dans l'intérêt du service, pour protéger les informations de l'administration dont la divulgation pourrait nuire au bon fonctionnement de ses tâches. Le non-respect de cette obligation, hormis dans les cas expressément prévus par la loi ou sous couvert de l'autorité dont dépend l'agent, l'expose à des sanctions disciplinaires.

L'administrateur fait preuve de prudence lors des échanges qu'il peut être amené à avoir sur les réseaux d'entraide afin de ne pas dévoiler des éléments techniques ou organisationnels qui pourraient être utilisés à l'encontre de l'institution.

3.3 Relation avec les utilisateurs

Les règles et procédures d'administration des systèmes d'information et de sécurité servent en priorité à la mise en œuvre, au maintien ou à l'amélioration de la qualité des prestations délivrées à l'utilisateur.

L'administrateur s'assure de la qualité du service rendu aux utilisateurs et contribue à leur soutien en liaison avec les autres intervenants, notamment par le transfert d'un minimum d'informations permettant aux utilisateurs d'user du système en condition normale et de faire appel, le cas échéant, à une assistance.

L'administrateur participe également à la sensibilisation des utilisateurs :

- en rappelant régulièrement les principes de la charte d'usage du système d'information ;
- en informant les utilisateurs des consignes techniques de sécurité à mettre en œuvre afin de préserver le système d'information ;
- en participant à la sensibilisation des utilisateurs aux usages raisonnés du numérique et aux risques encourus par l'institution et eux-mêmes ;
- 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 « **privé** » afin de faciliter le respect de l'intimité de sa vie privée.

3.4 Droits de l'administrateur

L'administrateur est informé par sa hiérarchie des implications légales de son travail.

L'administrateur ne peut être contraint à enfreindre la loi.

Il bénéficie d'une protection juridique vis à vis du refus d'obéir aux actions manifestement illégales commandées par sa hiérarchie ou de nature à compromettre gravement un intérêt public.

3.4.1 Actions autorisées de l'administrateur sur son périmètre

Dans le cadre du respect de la politique de sécurité du système d'information (PSSI) l'administrateur peut :

- mettre en place des moyens permettant de fournir des informations techniques d'administration de réseau ;
- 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 ;
- accéder, sur les systèmes qu'il administre, à tout type d'information, mais 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 ;
- établir des procédures de surveillance de toutes les tâches exécutées sur le matériel informatique utilisé, afin de déceler les violations ou les tentatives de violation de la présente charte et de la charte d'usage du système d'information, sous l'autorité de son responsable et en relation avec le RSSI.

Dans les cas où le maintien en condition de sécurité du système d'information considéré l'exige, l'accès aux dossiers ou mails revêtant la mention « privé » peut être opéré par les outils automatiques (ex. : antivirus) ou les administrateurs eux-mêmes.

Dans ce cas, l'accès aux dossiers ou courriels personnels de l'agent par l'administrateur doit se faire en présence de l'agent, sauf cas de force majeure. En tout état cause, tous les moyens nécessaires doivent être mis en œuvre pour informer l'agent préalablement à l'intervention de l'administrateur. Cette intervention n'autorise en aucune manière l'administrateur à révéler à quiconque le contenu des fichiers personnels, en dehors des exceptions et limites légales sus rappelées.

3.5 Devoirs de l'administrateur

L'administrateur doit :

- respecter les dispositions légales et réglementaires concernant le système d'information. Le doute entraîne la consultation de la chaine SSI ;
- se conformer à la politique de sécurité des systèmes d'information de l'établissement, appliquer les politiques d'exploitation de sécurité (PES) attachées aux systèmes d'information dont il a la charge et rendre compte de toute difficulté d'application.
  À défaut de PES, il applique les règles générales de sécurité correspondant à l'environnement d'exploitation prescrit ;
- respecter la confidentialité des informations auxquelles il accède lors de ses tâches d'administration quel qu'en soit le support et la nature ;
- 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 chaine SSI ou de l'utilisation d'outils automatiques, tels qu'antivirus ou inventaire logiciel, qui ne visent pas individuellement l'utilisateur ;
- 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 ;
- s'assurer de l'identité et de l'habilitation de l'utilisateur lors de la remise de tout élément du système d'information en collaboration avec le responsable fonctionnel ;
- répondre à toute consigne de surveillance, de recueil d'information ou d'audit émise par le RSSI.

En cas d'incident l'administrateur doit :

- le traiter en première priorité et prendre toute disposition nécessaire pour toute violation des règles SSI et tout incident de sécurité qu'il est amené à constater et en informer sans délai la chaine SSI ;
- prendre des mesures conservatoires si l'urgence l'impose.

Les principales actions d'administration sont consignées soit de manière automatique, soit de manière manuelle, afin que le cours des événements puisse être au besoin fidèlement retracé. L'administrateur tient en outre à jour la documentation technique et les configurations de tous les composants du système d'information. L'administrateur veille à ne pas porter atteinte à l'intégrité des fichiers de journalisation et ne désactive pas les mécanismes de traçabilité. En cas de force majeure seul le RSSI peut prendre l'initiative d'une désactivation temporaire.

L'administrateur veille à ce que les logiciels soient utilisés dans les conditions de licences souscrites. Dans le cadre de sa mission, il n'utilise que des logiciels conformes à la politique de sécurité de l'institution. Toute dérogation doit faire l'objet d'une autorisation préalable et explicite de son responsable hiérarchique et du RSSI de l'entité.

En cas de requête officielle des autorités judiciaires, l'administrateur remet toute information demandée, en lien avec son responsable hiérarchique.

Les informations issues des dispositifs dédiés à la capture et/ou l'enregistrement d'images ou de conversations à des fins de surveillance, de preuve, de formation ou

d'évaluation ne doivent être consultées que par le personnel habilité, formé et investi d'une mission de surveillance ou de contrôle, ce qui exclut le personnel administrateur.

Si un administrateur venait exceptionnellement à prendre connaissance du contenu des enregistrements pour des motifs légitimes de maintien en condition de sécurité du système, les principes exposés précédemment lui interdisent de divulguer les informations dont il aurait ainsi eu connaissance.

3.6 Traitement des dysfonctionnements et des incidents de sécurité

3.6.1 Généralités

Dans le cadre de ses fonctions, l'administrateur peut être alerté sur des dysfonctionnements ou des incidents de sécurité touchant le système d'information :

- sont appelées dysfonctionnements toutes les défaillances physiques ou logiques rencontrées sur le système, voire sur les servitudes indispensables à son bon fonctionnement. L'administrateur réagit alors selon les consignes propres au système concerné ;
- sont appelés incidents de sécurité tous les faits ou événements volontaires ou involontaires, issus d'un utilisateur légitime ou non, voire d'un système externe, et portant atteinte à la sécurité du système administré ou au respect de la loi.

Un administrateur constatant un incident de sécurité doit prendre immédiatement les mesures permettant :

- de faire cesser l'incident en cours et de se préserver d'éventuels effets ultérieurs selon les procédures mises en place et en cohérence avec le besoin opérationnel qui reste prioritaire ;
- de recouvrer le niveau de sécurité normal du système ;
- d'assurer la continuité de service, au besoin en mode dégradé.

Il rend compte sans délai à sa hiérarchie et à l'autorité fonctionnelle SSI des faits constatés et des actions de remédiation conduites.

Certains incidents pouvant déboucher sur des poursuites disciplinaires ou judiciaires, l'administrateur prend les mesures adaptées afin de préserver les éléments de preuve de l'acte malveillant.

3.6.2 La préservation des preuves

La preuve est la démonstration de la réalité d'un fait, d'un état, d'une circonstance ou d'une obligation. Elle a pour finalité soit d'apporter des éléments contradictoires aux faits contestés, soit d'établir les allégations et ainsi d'aider le juge à se forger une intime conviction, ou l'autorité hiérarchique à apprécier l'opportunité d'une éventuelle sanction ou action en justice.

L'administrateur doit agir rapidement, et si possible en présence d'un représentant de l'autorité fonctionnelle SSI en qualité de témoin, afin de fixer la preuve dans le temps et d'éviter sa disparition ou son altération. À ce titre, les actions suivantes sont à mener sans délai :

- déconnecter le serveur, le poste de travail ou l'élément de stockage du réseau afin d'éviter toute action d'effacement ou de modification de preuve postérieure à la découverte du délit. En fonction des besoins opérationnels, la continuité de service devra être assurée, le cas échéant, par la mise en œuvre d'un mécanisme de secours ;
- éviter, dans la mesure du possible, d'éteindre l'équipement incriminé (cette opération pourrait avoir pour effet d'effacer les traces présentes en mémoire) ; si la machine doit cependant être éteinte, ne pas utiliser la fonction d'extinction du système mais débrancher le cordon d'alimentation ;
- verrouiller le(s) compte(s) du (des) utilisateur(s) incriminé(s), ainsi que l'accès aux comptes de messagerie ;
- ne pas connecter de supports amovibles sans nécessité afin de ne pas générer de traces parasites ;
- restreindre l'accès physique à l'élément incriminé de manière à ce que personne ne modifie sa configuration avant l'intervention des services compétents.
- noter, sur un journal de bord, l'ensemble des constatations faites et des actions effectuées de manière à assurer une traçabilité et un historique de l'incident en précisant :
    - les dates et heures du système et réelles, celles-ci pouvant différer ;
    - le nom des fichiers ou commandes exécutés ainsi que les identifiants et mots de passe utilisés si des actions d'administration sont nécessaires ;
- préserver le plus grand nombre d'informations pertinentes pouvant compléter les investigations tels que supports de sauvegardes récentes ou journaux d'évènements.
- Dans tous les cas, il y a lieu d'agir avec la plus grande discrétion et respecter le principe de la présomption d'innocence.

4 RESPECT DE LA LÉGISLATION ET DE LA PRÉSENTE CHARTE

L'administrateur d'un système d'information s'engage à respecter en toute circonstance la réglementation en vigueur, ainsi que la présente charte et la charte régissant l'usage du système d'information par les personnels de l'académie d'Aix-Marseille.

En cas de non-respect des textes en vigueur ou des dispositions de la présente charte, l'administrateur sera tenu pour responsable de ses actes et encourra les sanctions pénales, civiles, administratives et disciplinaires prévues par les textes applicables.

Tout document relatif aux règles, procédures, conditions ou missions d'administration d'un système d'information doit être conforme aux principes de la présente charte.

5 STATUT DE LA CHARTE

Le comité technique académique a examiné les dispositions de cette charte lors de sa séance du 29-05-2017.

Sa date d'entrée en vigueur est fixée au 01-09-2017.

Cette charte est publiée au bulletin académique BA n°.....

6 ENGAGEMENT INDIVIDUEL DE RESPONSABILITÉ

Chaque administrateur d'un système d'information est tenu d'en prendre connaissance et s'engage à la respecter par la signature d'un engagement individuel de responsabilité.

L'engagement individuel de responsabilité est signé en deux exemplaires par l'administrateur et cosigné par son supérieur hiérarchique. Un exemplaire est conservé au sein du service ou établissement et l'autre par l'administrateur lui-même.

Les principales dispositions légales et réglementaires en vigueur dans le domaine de la sécurité des systèmes d'information sont énumérées dans l'annexe juridique.

6.1 Exemplaire conservé par l'administrateur

ENGAGEMENT INDIVIDUEL DE RESPONSABILITÉ DE L'ADMINISTRATEUR DE SYSTÈME D'INFORMATION

Je soussigné, ... déclare avoir pris connaissance de la **charte des administrateurs du système d'information de l'académie d'Aix-Marseille** et m'engage à la respecter.

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

ENGAGEMENT DU SUPÉRIEUR HIÉRARCHIQUE DIRECT

Je soussigné, ... agissant en tant que supérieur hiérarchique direct de ..... déclare avoir pris connaissance de la **charte des administrateurs du système d'information de l'académie d'Aix-Marseille** et m'engage à en respecter les termes et limites définies.

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

[page blanche]

6.2 Exemplaire conservé par le service

ENGAGEMENT INDIVIDUEL DE RESPONSABILITÉ DE L'ADMINISTRATEUR DE SYSTÈME D'INFORMATION

Je soussigné, ... déclare avoir pris connaissance de la **charte des administrateurs du système d'information de l'académie d'Aix-Marseille** et m'engage à la respecter.

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

ENGAGEMENT DU SUPÉRIEUR HIÉRARCHIQUE DIRECT

Je soussigné, ... agissant en tant que supérieur hiérarchique direct de ..... déclare avoir pris connaissance de la **charte des administrateurs du système d'information de l'académie d'Aix-Marseille** et m'engage à en respecter les termes et limites définies.

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