Version 1.0 du 29 novembre 2024

Charte de l’administrateur des systèmes d’information et de communication de l’Institut Mines-Télécom et ses écoles

Approuvée par le Conseil d’administration de l’Institut Mines-Télécom le 29 novembre 2024

Annexe 2 du Règlement intérieur de l’Institut Mines-Télécom

Institut Mines-Télécom

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ARTICLE 1 : PRÉAMBULE

La présente charte constitue une annexe du règlement intérieur de l'Institut Mines-Télécom, au même titre que la charte de l'utilisateur des systèmes d'information et de communication de l'Institut Mines-Télécom et de ses écoles.

Les administrateurs disposent de droits étendus par rapport aux utilisateurs pour les besoins de leur mission. Ces droits 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 donner lieu à des mesures disciplinaires ou des poursuites judiciaires.

En raison de leurs prérogatives, ces personnels ont un rôle essentiel, requérant discrétion et diplomatie : leur démarche doit être exemplaire et impartiale. 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 des systèmes d'information et de communication et la confiance des usagers dans ces derniers supposent 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.

ARTICLE 2 : DÉFINITIONS

Au sens de la présente charte :

les « **systèmes d'information et de communication de l'IMT »** recouvrent l'ensemble des ressources matérielles, logicielles, applications, bases de données et réseaux de télécommunications de l'IMT ou que l'IMT met à la disposition de ses utilisateurs. Ils sont aussi constitués des dispositifs numériques nomades privés connectés à l'IMT.

Les directeurs ainsi que leurs chefs de service sont responsables de leurs données métier.

Le terme d'« **administrateur** » recouvre les personnes expressément désignées comme telles par l'IMT ou par le prestataire de l'IMT , ayant des droits d'accès étendus aux systèmes d'information et de communication de l'IMT 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. Un administrateur peut être un membre du personnel de l'IMT ou un membre du personnel d'un prestataire de l'IMT.

ARTICLE 3 : CHAMP D'APPLICATION

La présente charte précise le cadre légal, réglementaire et déontologique dans lequel doivent s'inscrire les actions d'administration des systèmes d'information et de communication de l'IMT.

ARTICLE 4 : DÉSIGNATION ET COMPÉTENCES DES ADMINISTRATEURS DE L'IMT

Section 4.1 : Désignation des administrateurs

Les directeurs et chefs de service tiennent à jour, concernant leur périmètre de responsabilités, la liste des profils d'accès en administration et des services qui leur sont associés, en précisant la nature et le périmètre du champ d'intervention.

Lorsqu'il s'agit d'entreprises prestataires, ces éléments sont précisés dans le contrat signé avec ces derniers.

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 et de communication (RSSI) de l'entité concernée.

Les profils sont revus à fréquence régulière et actualisés au moins une fois annuellement, le cas échéant.

Le principe appliqué est systématiquement l'optimisation du nombre d'administrateurs afin de diminuer le risque d'exploitation de ces profils, tout en assurant la continuité de service.

Les administrateurs ainsi désignés doivent disposer des compétences mentionnées ci-après.

Section 4.2 : Compétences

Préalablement à la désignation d'un administrateur et tout au long de ses fonctions, l'IMT s'assure que ce dernier dispose des compétences requises par la fonction dans les domaines relatifs :

- aux ressources matérielles et logicielles gérées ;
- aux lois et règlements applicables aux systèmes d'information et de communication administrés, leurs évolutions et, plus généralement, le domaine juridique des nouvelles technologies ;
- à la Politique de Sécurité des Systèmes d'Information de l'IMT ;
- à l'application à ces systèmes des mesures de sécurité et des mesures d'urgence ;
- au suivi des vulnérabilités du (des) système(s) servi(s), des menaces pesant sur eux et des méthodes d'attaques de ces systèmes ;
- au suivi du niveau d'alerte SSI et de l'actualité de la menace ;
- au respect des réglementations auxquelles il est soumis (exemple : RGPD)

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

Les mêmes obligations s'appliquent aux prestataires de l'IMT chargés d'administrer des systèmes d'information et de communication de l'IMT, à savoir prendre en charge les besoins de formation et veiller au maintien de compétences.

ARTICLE 5 : 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 l'intérêt public.

Dans le respect de la Politique de Sécurité des Systèmes d'Information de l'IMT, 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 des Systèmes 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 hiérarchique et en relation avec le RSSI.

L'administrateur peut prendre connaissance de fichiers ou données identifiées comme personnels dans les seules conditions visées à la section 6.6.

ARTICLE 6 : DEVOIRS DES ADMINISTRATEURS

L'administrateur met en œuvre la Politique de Sécurité des Systèmes d'Information de l'IMT. Il déploie les mesures qui s'imposent sur son périmètre. Il informe le RSSI de tout incident de sécurité dès sa constatation.

Section 6.1 : Principe de maitrise des droits d'administration

Lorsque cela est possible, l'IMT met en place des plateformes de gestion des accès avec des droits étendus, afin d'assurer la traçabilité et l'imputabilité des actes d'administration. À défaut, il 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 (SSH, FIDO2) ou les mécanismes forts d'authentification (LAPS ou double authentification) doivent alors être privilégiés.

Lorsque l'authentification est réalisée au moyen d'un mot de passe, celui-ci doit être suffisamment long et complexe. Il est recommandé de le changer 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.

Section 6.2 : 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 et d'exploitation définies.

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.

Il recueille l'autorisation de sa hiérarchie et s'assure de la communication de cette interruption, auprès des utilisateurs impactés via les canaux de communication dont il dispose et dans la limite du niveau de sensibilité de cette information (exemples de classification de la sensibilité applicables : TLP, PAP).

Section 6.3 : Secret professionnel

Les administrateurs, en tant que dépositaires de renseignements concernant ou intéressant des personnes physiques, 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 agent 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.

Section 6.4 : Discrétion professionnelle

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'administrateur, 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 se rapportant à l'IMT.

Section 6.5 : 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 des systèmes d'information et de communication ;
- 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'IMT 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.

Section 6.6 : Accès aux fichiers et données personnelles des utilisateurs

L'administrateur peut accéder aux fichiers, dossiers et données des utilisateurs des systèmes d'information et de communication de l'IMT identifiés comme personnels en l'absence de l'utilisateur en cas d'évènement ou de risque particulier pour l'IMT, notamment si le maintien en condition de sécurité du système d'information l'exige. Tous les moyens nécessaires doivent être mis en œuvre pour informer l'agent préalablement à l'intervention de l'administrateur, sauf cas de force majeure et sauf dans les situations où l'information préalable de l'utilisateur est incompatible avec l'objectif de l'opération envisagée. Dans tous les cas, l'accès à ces éléments personnels doit être préalablement autorisé par la chaîne SSI.

Si l'accès aux éléments personnels d'un utilisateur n'est pas justifié par un évènement ou risque particulier pour l'IMT, l'utilisateur doit être présent ou avoir été invité à être présent.

L'intervention de l'administrateur ne l'autorise en aucune manière à révéler à quiconque le contenu des fichiers personnels, en dehors des exceptions et limites légales.

Les outils automatiques (ex : antivirus ou inventaires logiciels) peuvent également accéder aux fichiers, dossiers et données des utilisateurs des systèmes d'information et de communication de l'IMT identifiés comme personnels en l'absence de l'utilisateur et sans que celui-ci en soit préalablement informé lorsqu'ils ne visent pas individuellement l'utilisateur. L'administrateur veille à ce que ces outils n'entravent pas le bon fonctionnement des systèmes d'information et de communication de l'IMT.

Section 6.7 : Autres devoirs de l'administrateur

L'administrateur doit :

- respecter les dispositions légales et réglementaires concernant le système d'information. Le doute impose la consultation de la chaîne SSI ;

- se conformer à la Politique de Sécurité des Systèmes d'Information de l'IMT, 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 quels qu'en soient le support et la nature ;
- 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 des systèmes d'information et de communication en collaboration avec le responsable hiérarchique ;
- répondre à toute consigne de surveillance, de recueil d'information ou d'audit émise par le RSSI.

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 des Systèmes d'Information de l'IMT. 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 les administrateurs.

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.

ARTICLE 7 : TRAITEMENT DES DYSFONCTIONNEMENTS ET INCIDENTS DE SÉCURITÉ

Section 7.1 : 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 ;
- 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 avec les moyens dont il dispose, et de se préserver d'éventuels effets ultérieurs 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.

Dans la limite des moyens de communication dont il dispose, il rend compte sans délai à sa hiérarchie et au RSSI dont il dépend, à défaut à l'autorité qualifiée de la SSI (AQSSI) 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.

Section 7.2 : 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 dès que possible, consigner par écrit la décision justifiée auprès d'un représentant de l'AQSSI en qualité de témoin (exemple : le RSSI ou son suppléant, à défaut le DSI), et si possible en sa présence, 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.

ARTICLE 8 : RESPECT DE LA LÉGISLATION ET DE LA PRÉSENTE CHARTE

L'administrateur d'un système d'information et de communication s'engage à respecter en toute circonstance la réglementation en vigueur, ainsi que la présente charte et la charte régissant l'usage des systèmes d'information et de communication par les personnels de l'IMT.

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.

GLOSSAIRE

[AQSSI] : Autorité Qualifiée pour la Sécurité des Systèmes d'Information. L'AQSSI est la personne physique juridiquement responsable pour sa structure, de la sécurité des systèmes d'information. Sa responsabilité ne peut être déléguée. L'AQSSI désigne un RSSI pour l'assister dans ses fonctions. La nomination de l'AQSSI est liée à l'arrêté du 13 décembre 2016 portant désignation des autorités qualifiées pour la sécurité des systèmes d'information dans les services d'administration centrale, les services déconcentrés, les organismes et établissements sous tutelle des ministères chargés des affaires sociales.

[PSSI] : Politique de Sécurité des Systèmes d'Information.

[RSSI] : Responsable de la sécurité des systèmes d'information et de communication. Il est nommé et mandaté par l'AQSSI pour mettre en place la politique de sécurité des systèmes d'information. Le RSSI est le responsable opérationnel.