Charte des administrateurs du système d'information de l'UTC

Préambule

Les différents systèmes d'information de l'UTC (système de gestion, infrastructure réseau, infrastructure de virtualisation, informatique de la BUTC…) que l'on appellera dans la suite de ce document « système d'information (SI) » constituent un élément indispensable à l'accomplissement des missions et des activités de l'université. Il en résulte que la bonne administration du système d'information et des données qu'il supporte ou traite est une condition nécessaire à la réalisation de ces missions et activités de manière satisfaisante.
Les personnes chargées de l'administration de tout ou partie du système d'information, appelées « administrateurs du système d'information », disposent de droits d'accès étendus. Elles peuvent alors être amenées à accéder à des informations ou données présentant un caractère confidentiel[1]. Elles sont également amenées à effectuer régulièrement des actions sensibles.

En raison de leurs prérogatives, les administrateurs ont un rôle essentiel, requérant responsabilité et discrétion. Leur démarche se doit d'être impartiale et respectueuse des droits fondamentaux des utilisateurs (protection des données personnelles, respect de la vie privée, secret des correspondances…). 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 des administrateurs du système d'information de l'UTC est destinée à préciser les droits et les devoirs de toutes personnes chargées de la gestion d'éléments du système d'information de l'établissement. Elle n'a pas pour but de décrire les métiers d'administrateurs système, réseau ou de systèmes d'information.

Par « l'établissement », on désigne l'UTC.

I. Définitions et acronymes

I.1 Système d'information (SI)

Le système d'information comprend l'ensemble des moyens matériels, logiciels, applications, bases de données, réseaux de télécommunication, et des informations et données qui y sont traitées[2] ou hébergées.
Le système d'information inclut tout élément contribuant à :

- la gestion des informations de l'établissement,
- la gestion des informations de partenaires de l'UTC dont l'administration ou la maintenance ont été confiées à l'UTC par voie de convention.

Les éléments suivants font donc partie du système d'information (liste non exhaustive) : les serveurs, le réseau, physique ou logique, et les éléments le constituant, les postes de travail individuels, fixes et portables, les ordinateurs personnels et les téléphones mobiles au sein de l'établissement, dès lors qu'ils sont connectés au réseau de l'UTC ou lorsqu'ils sont identifiés par leur propriétaire comme terminaux hébergeant des activités UTC, les moyens de stockage nomade (clés USB, disques externes…), les bases de données, les systèmes d'exploitation, les applications informatiques, l'infrastructure de téléphonie, l'infrastructure de vidéoprotection, l'infrastructure de contrôle d'accès…

[1] Données sur des espaces personnels ou partagés, données à caractère personnel, données privées, données sensibles de recherche, contrats, brevets…
Donnée à caractère personnel : donnée permettant d'identifier une personne physique de manière directe ou indirecte, y compris par recoupement. Les traces informatiques (ou « logs ») sont des données à caractère personnel et doivent de ce fait être manipulées dans le respect des droits des personnes, conformément au RGPD et à la loi du 6 janvier 1978 dite « informatique et libertés ».

[2] Traitement : toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

I.2 Administrateur du système d'information

Le terme administrateur désigne toute personne employée ou non par l'établissement, à laquelle a été confiée la responsabilité permanente ou ponctuelle de l'exploitation, de l'administration, de la maintenance, de la mise en œuvre, du déploiement ou du développement d'un élément du système d'information. Une personne à qui a été conférée une telle responsabilité est désignée dans ce document par le terme « administrateur ».
Il possède des droits étendus dans la limite des nécessités de ses missions. Dans le cadre de son activité, il peut être amené à avoir accès aux informations d'autres utilisateurs, parfois confidentielles.
L'ensemble des éléments sur lesquels s'exerce la responsabilité d'un administrateur constitue son périmètre d'activité.

I.3 Responsable de la sécurité des systèmes d'information (RSSI)

Le RSSI, désigné par l'Autorité Qualifiée de Sécurité du SI (AQSSI)[3], est le relais entre celui-ci, les responsables fonctionnels et les administrateurs du système d'information.

I.4 Politique de sécurité des systèmes d'information de l'état(PSSIE)

La PSSIE formalise, dans un ensemble de documents, une liste de mesures de sécurité à mettre en œuvre.

I.5 Violation de données

Par violation de données, on entend une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données[4].

II. Droits et devoirs de l'administrateur

L'administrateur est chargé de garantir la disponibilité, l'intégrité, la confidentialité, la sécurisation et la traçabilité des données échangées ou mises à disposition des utilisateurs, dans la limite des moyens alloués. Dans le cadre de sa mission, l'administrateur peut potentiellement accéder à l'ensemble des informations contenues dans le système d'information.
Toutefois, la mission de l'administrateur s'exerce dans un cadre réglementaire et éthique strict. Aucune exploitation des informations dont un administrateur pourrait prendre connaissance pendant l'exercice de ses missions, à des fins autres que celles liées à ses missions, et qui aurait pour conséquence de violer une réglementation, en particulier relative aux droits et libertés de l'utilisateur, ne saurait être entreprise, que ce soit à sa propre initiative ou sur ordre hiérarchique[5].
Les pouvoirs étendus dont disposent les administrateurs leur confèrent ainsi des droits et des devoirs spécifiques.

II.1 Droits de l'administrateur

L'administrateur a le droit, dans le cadre strict des missions qui lui sont confiées et du respect des mesures de sécurité de la PSSIE :

- d'être informé par sa hiérarchie des implications légales de son travail,
- d'accéder aux informations nécessaires à l'accomplissement de sa mission, en s'interdisant scrupuleusement de divulguer ces informations, et en s'efforçant de ne pas les altérer — tant que la situation ne l'exige pas —,
- de mettre en place :
    - des moyens permettant de fournir des informations techniques d'administration des éléments du système d'information à sa charge (métrologie, outils de gestion et de corrélation de journaux d'évènements…)
    - des procédures de surveillance et de protection des données, des réseaux, des systèmes et des applications afin de déceler des anomalies,
    - toutes procédures appropriées pour vérifier la bonne application des règles de sécurité de la PSSIE, en utilisant des outils autorisés,

  en accord avec la PSSIE, dans le respect des dispositions réglementaires[6] et sous l'autorité de son responsable fonctionnel,

[3] L'AQSSI est le directeur de l'UTC.
[4] Article 4, règlement général sur la protection des données, règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016.
[5] Article 28, loi du 13 juillet 1983, relative au statut des fonctionnaires, mais aussi applicable aux agents non titulaires.
[6] Par exemple, pour tout traitement de données à caractère personnel, chaque utilisateur doit être préalablement informé, notamment des finalités poursuivies, de la base légale du dispositif (obligation issue du Code du travail ou intérêt légitime de l'employeur), des destinataires des données, de la durée de conservation

- de prendre toute mesure conservatoire si l'urgence l'impose, telles que restriction de connectivité, suppression de fichiers (après sauvegardes sur support isolé) s'il estime qu'ils pourraient porter atteinte à la sécurité, l'intégrité, la confidentialité ou la disponibilité d'un ou plusieurs composants du système d'information.

L'administrateur n'a pas le droit d'intervenir sur un composant hors du système d'information de l'établissement et hors du système d'information de partenaires dont l'administration ou la maintenance ont été confiées à l'établissement par convention, sauf à l'isoler du reste de l'établissement en cas de besoin.

II.2 Devoirs de l'administrateur

L'administrateur a pour devoirs :

- **de respecter les dispositions légales et réglementaires concernant le système d'information,**
- **de respecter et préserver la confidentialité** des informations auxquelles il accède, quel qu'en soit le support, en particulier les données à caractère personnel, les fichiers utilisateurs, les traces sur le réseau, les courriers électroniques, les mots de passe, les sorties imprimantes, les traces des activités des utilisateurs…
- **de n'effectuer des accès aux contenus identifiés comme privés** qu'avec l'accord écrit de l'utilisateur, à l'exception des cas d'atteinte à la sécurité, sous couvert d'une autorisation du RSSI ou de l'AQSSI ou d'atteinte à la disponibilité d'informations indispensables à la continuité du service, sous couvert d'une autorisation de l'AQSSI. Lorsque l'administrateur effectue un accès aux contenus identifiés comme privés, l'utilisateur peut être présent.
  Cette obligation ne s'applique pas lors de l'utilisation d'outils automatiques qui ne ciblent pas individuellement l'utilisateur (antivirus, inventaire logiciel, logiciel de sauvegarde…).
- **d'agir avec transparence** : l'administrateur doit informer l'utilisateur de l'étendue des accès aux informations dont il dispose techniquement en raison de sa fonction, de tout accès à son environnement de travail individuel (intervention locale ou prise de main à distance) et des motifs l'y autorisant conformément à l'exercice de ses missions (sauf dans le cas où la discrétion des opérations est imposée par les autorités judiciaires).
  Il informe également l'utilisateur de toute opération tendant à accéder à ses courriels ou à ses fichiers sur son poste de travail ou sur un volume distant, et des motifs l'y autorisant conformément à l'exercice de ses missions (sauf dans le cas où la discrétion des opérations est imposée par les autorités judiciaires).
  Il doit inviter l'utilisateur à classer ses données personnelles et professionnelles, chaque fois que cela est possible, avant chaque intervention sur son poste de travail, afin de respecter l'intimité de la vie privée de l'utilisateur et de délimiter plus facilement le cadre de l'intervention.
- **d'ajuster avec proportionnalité** ses interventions : l'accès direct aux informations de l'utilisateur ne saurait être justifié que dans le cas où le bon fonctionnement des systèmes informatiques ne pourrait être assuré par des moyens moins intrusifs, et si l'utilisateur en a été informé,
- **de s'assurer de l'identité et de l'habilitation de l'utilisateur** lors de la remise de tout élément du système d'information (information, fichier, compte d'accès, matériel...), en collaboration avec le responsable fonctionnel,
- **de se conformer** à la politique de sécurité du système d'information (PSSIE),
- **de refuser de répondre** à une demande qui aurait pour conséquence de lui faire commettre une infraction (droit à la vie privée, droit au secret des correspondances, RGPD[7], loi « informatique et libertés »…),
- **de veiller à la déclaration** des traitements de données conformément à la réglementation en vigueur,
- **de traiter en première priorité** toute violation des règles de sécurité des systèmes d'information (SSI) et tout incident de sécurité qu'il est amené à constater en mettant en œuvre les directives de traitement de l'incident et en se conformant à la chaine d'alerte,
- **de respecter la chaine d'alerte** décrite ci-dessous,
- **de sensibiliser les utilisateurs** aux bonnes pratiques de sécurité numérique, assisté par le responsable fonctionnel**.**

---

des données, de son droit d'opposition pour motif légitime, de ses droits d'accès et de rectification, de la possibilité d'introduire une réclamation auprès de la CNIL.

Par ailleurs, dans le cas de la mise en œuvre d'un dispositif de contrôle de l'activité, les instances représentatives du personnel doivent être informées ou consultées avant la mise en œuvre.

[7] Règlement général sur la protection des données, règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016.

III. Chaine d'alerte

L'administrateur doit informer immédiatement le RSSI de l'université ou son suppléant de toute tentative d'intrusion sur un système, ou de tout comportement d'utilisateur pouvant compromettre la sécurité du système d'information de l'université, dont il aurait eu connaissance pendant l'exercice de ses missions.
Il informe sans tarder le RSSI de l'université ou son suppléant de toute violation des règles de sécurité des systèmes d'information (SSI) et tout incident de sécurité qu'il est amené à constater ou traiter.
Il informe aussi immédiatement son responsable hiérarchique dès lors qu'il en a connaissance, d'actions illégales ou de données illicites sur les composants du système d'information dont il a la responsabilité.
L'administrateur peut ainsi être conduit à communiquer des informations confidentielles ou soumises au secret des correspondances dont il aurait eu connaissance, si elles concourent au dysfonctionnement ou à la compromission de la sécurité de tout ou partie du système d'information, ou si elles tombent dans le champ d'application de l'article 40 du code de procédure pénale[8].
Enfin, il informe sans tarder le délégué à la protection des données de l'UTC, de toute violation de données.

IV Cadre juridique

Il est fourni à titre indicatif et propose un cadre général à l'administrateur, mais ne présuppose pas des évolutions réglementaires et jurisprudentielles ultérieures dont l'administrateur sera explicitement informé par sa hiérarchie.

- Droit au respect de la vie privée[9]
  S'applique à toutes données notamment le contenu des fichiers, les courriels…
- Droit au secret des communications électroniques, lequel ne peut être levé qu'avec son accord
  Application : données personnelles relatives à la consultation de sites Internet de l'utilisateur (historique des navigations, signets, mémoire cache).
- Droit au secret des correspondances[10]
  Application au courriel en particulier.
- Règlement général sur la protection des données (RGPD)
  En application depuis le 25 mai 2018, il encadre le traitement des données personnelles sur le territoire de l'Union européenne.
- Loi du 6 janvier 1978 dite loi « informatique et libertés »
- Article 40 du code de procédure pénal

Engagement sur l'honneur

L'administrateur certifie avoir pris connaissance de la présente charte et s'engage sur l'honneur à en respecter les dispositions.

Fait le 14/11/2023 à 15:03

Faire précéder de la mention « lu et approuvé ».
(Nom, Prénom, Signature)

Lu et approuvé

Hugo Heuzebroc

[8] « Toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs ».
[9] Article 9 du Code civil, article 8 de la Convention européenne des droits de l'homme.
[10] Infraction prévue par l'article 432-9 du Code pénal, passible de 3 ans de prison et de 45 000 € d'amende.