CHARTE DE DÉONTOLOGIE DES ADMINISTRATEURS DU SYSTÈME D'INFORMATION DE L'UNIVERSITÉ BOURGOGNE EUROPE

5 – Déontologie des administrateurs

s'applique à :

Tout personnel, étudiant et usager du système d'information de l'Université Bourgogne Europe (UBE)
Ci-dessous désignés par l'« utilisateur »

Par :

L'Université Bourgogne Europe
Ci-dessous désignée par « l'Université » ou « UBE »

Charte présentée au CSA du 11/06/2025

Charte votée par le Conseil d'Administration (CA) de l'UBE le 08/07/2025. Cette charte vaut pour règlement intérieur.

ENT : Environnement Numérique de Travail

https://ent.ube.fr

Préambule

La fourniture des services liés aux technologies de l'information et de la communication s'inscrit dans la mission de service public de l'Enseignement Supérieur et Recherche (ESR).

Pour en assurer le fonctionnement, des agents employés spécifiquement (dénommés « administrateurs ») sont amenés à effectuer diverses opérations techniques pour fournir un service de qualité aux utilisateurs.

Ces opérations peuvent conduire les administrateurs à prendre connaissance d'informations de nature confidentielle, et doivent faire ceci en respectant les droits fondamentaux de l'utilisateur (protection des données personnelles, vie privée, secret des correspondances).

Aussi après avoir précisé le cadre technique de l'intervention des administrateurs, cette charte définira le cadre juridique de l'intervention des administrateurs.

SOMMAIRE

Article 1. Rôle et responsabilité – définition des personnes 4

1.1 L'administrateur systèmes 4

1.2 Le Chargé de Sécurité des Systèmes d'Information (CSSI) 5

1.3 Le Responsable de la Sécurité des Systèmes d'Information (RSSI) 5

Article 2. Droits de l'administrateur 5

Article 3. Devoirs de l'administrateur 5

3.1 Les missions ..... **Erreur ! Signet non défini.**

3.1.1 Assurer un service de qualité aux utilisateurs 6

3.1.2 Transparence des opérations effectuées 6

3.1.3 Chaîne d'alerte 7

3.1.4 Sensibilisation des utilisateurs 7

3.2 Les moyens 7

3.2.1 Les sauvegardes automatiques 7

3.2.2 La métrologie en temps réel 8

3.2.3 La traçabilité des opérations informatiques 8

Article 4. Cadre juridique de l'intervention 8

4.1 Respect de la loi relative à l'informatique, aux fichiers et aux libertés, RGPD 9

4.2 Définitions 9

4.2.1 Les obligations spécifiques de l'administrateur, responsable du fichier 9

4.2.2 Les conditions de collecte des données et de traitement 9

4.2.3 Précautions particulières lors du traitement de données personnelles 10

4.2.4 Accès aux données personnelles de l'utilisateur sur son poste de travail 10

4.3 Obligation de confidentialité et secret professionnel 10

Article 5. Engagements 11

Introduction

La présente charte constitue une annexe de la charte du numérique de l'Université Bourgogne Europe. Elle est librement consultable via l'environnement numérique de travail de l'Université Bourgogne Europe, dénommée UBE. Elle engage pleinement la responsabilité de l'agent en cas d'infraction, ou de complicité d'infraction, à la règlementation en vigueur et au règlement intérieur de l'université.

Article 1. Rôle et responsabilité – définition des personnes

1.1 L'administrateur système

Le terme « administrateur » désigne tout agent ayant pour mission d'assurer le bon fonctionnement ou la sécurité des ressources des systèmes d'information placées sous sa responsabilité dont, notamment, les serveurs, les équipements réseau, les équipements de sécurité, les applications, les bases de données ou les postes de travail.

La présente charte s'adresse à tout administrateur, quel que soit son statut : titulaire ou contractuel, ainsi que tout consultant ou prestataire.

Pour l'exécution de sa mission, l'administrateur dispose de droits d'accès privilégiés susceptibles de lui permettre l'accès à des informations, tels que des courriels, des fichiers, des données de connexion - confidentielles ou non - à caractère privé ou professionnel, dont il n'est ni le destinataire, ni l'auteur, ni le propriétaire.

Ces droits d'accès privilégiés lui permettent aussi d'entreprendre des actions potentiellement dangereuses pour les systèmes d'information tels que, par exemple, la modification ou le contournement de mécanismes de protection, la création ou la modification de comptes utilisateurs, la destruction ou la modification de fichiers.

L'administrateur est tenu au secret professionnel et soumis à l'obligation de discrétion professionnelle, il exerce ses missions dans le respect des prescriptions règlementaires régissant son statut, excluant de fait toute utilisation de ses droits d'accès privilégiés à des fins personnelles.

L'administrateur systèmes, réseaux et systèmes d'information est la personne, à laquelle a été confiée la responsabilité d'un système informatique, d'un réseau, d'équipements de téléphonie, de la maitrise d'œuvre d'application ou d'un traitement de données.

Les administrateurs sont donc autant de personnes différentes qui interviennent sur plusieurs éléments d'un système informatique (liste non exhaustive) :

- les postes de travail individuels ;
- les bases de données, les systèmes d'exploitation du domaine ;
- le réseau, les applications (serveur/client) ;
- la téléphonie.

L'ensemble des éléments sur lesquels s'exerce cette responsabilité constitue le périmètre d'activité de l'administrateur.

1.2 Le Chargé de Sécurité des Systèmes d'Information (CSSI)

Le Chargé de Sécurité du Système d'Information (CSSI) est la personne relais du Responsable de Sécurité du Système d'Information (RSSI) de l'établissement pour son entité. Suivant le périmètre de l'entité, un ou plusieurs CSSI peuvent être nommés.
De par son rôle dans la chaine de sécurité du système d'information, il pourra être amené à avoir accès à des informations des autres utilisateurs, informations parfois confidentielles.
Les règles de déontologie définies pour l'administrateur s'entendent également pour le CSSI.

1.3 Le Responsable de la Sécurité des Systèmes d'Information (RSSI)

Le RSSI (responsable de la sécurité des systèmes d'information) est chargé de la définition et de la mise en œuvre de la politique de sécurité de l'établissement. Il possède en outre un rôle stratégique d'information, de conseil et d'alerte de la direction générale sur les risques en matière de sécurité informatique.
Les règles de déontologie définies pour l'administrateur s'entendent également pour le RSSI.

L'ensemble de ces personnes sont désignées ci-dessous par « Administrateur »

Article 2. Droits de l'administrateur

Dans le cadre de ses missions, un administrateur a le droit :

- d'interrompre le fonctionnement de tout équipement, logiciel ou matériel, qui compromettrait la sécurité ou le bon fonctionnement d'un - ou d'un ensemble de – système(s) d'information ;
- d'utiliser des données de connexion et d'accéder à des informations privées professionnelles à des fins de diagnostic, de vérification, de métrologie, de statistiques ou en cas d'anomalie ou d'incident ;
- de prendre les mesures adéquates afin de prévenir tout risque de sécurité tel que virus, intrusion ou vol de données, destruction de données ou contournement de la politique de sécurité.

Article 3. Devoirs de l'administrateur

Dans le cadre de ses missions, un administrateur :

- ne prend pas connaissance de données personnelles d'utilisateurs - sauf en cas de nécessité sur demande formelle AQSSI, DGS, FSD, sur demande formelle de l'utilisateur lui-même - et n'autorise quiconque à y accéder, sauf cas particulier prévus par la loi ;
- respecte les dispositions mentionnées dans la charte de bon usage des moyens numériques auxquelles sont soumis les administrateurs dans l'exercice de leurs missions, en particulier sur le

traitement des informations privées, sur la messagerie, sur le réseau Internet, sur la traçabilité, sur les mesures de contrôle et l'obligation d'information des utilisateurs ;

- respecte scrupuleusement la confidentialité des informations auxquelles il a accès et met en œuvre des mesures visant à assurer leur non-divulgation ;
- s'assure, avec le délégué à la protection des données (DPO) désigné, que la mise en œuvre du traitement respecte la règlementation sur la protection des données à caractère personnel ;
- informe le Responsable de la Sécurité des Systèmes d'Information (RSSI) de tout incident de sécurité ou toute faille de sécurité dont il pourrait avoir connaissance et respecte la chaine fonctionnelle de sécurité SI ;
- n'utilise ses droits d'accès privilégiés que ponctuellement et exclusivement pour les activités et les besoins directement liés à ses missions, et en aucun cas à des fins personnelles ;
- agis dans le sens d'une meilleure sécurité, dans l'intérêt de l'établissement et des utilisateurs ;
- Tout nouveau projet d'envergure mobilisant des moyens humains ou financiers importants, qu'il s'agisse de la mise en place d'une application, du lancement d'un développement ou tout projet qui utilise les outils, informations, bases de données qui sont hébergées au datacenter, doit être déclaré via une fiche projet accessible depuis l'ENT. Cette déclaration permet notamment de vérifier l'usage d'outils, de données ou de services hébergés au Datacenter, et d'éviter les redondances avec des projets existants ou en cours de déploiement.

3.1 Les missions

3.1.1 Assurer un service de qualité aux utilisateurs

Les administrateurs ont la charge de la bonne qualité du service fourni aux utilisateurs dans la limite des moyens alloués. Ils ont aussi le devoir d'assurer l'intégrité, la disponibilité et la confidentialité des données échangées ou accessibles depuis le réseau informatique de l'université.
Aussi ils ont le droit :

- d'entreprendre toute démarche nécessaire au bon fonctionnement des ressources informatiques de l'université, et d'accéder à tout type d'information nécessaire à l'accomplissement de leur mission ;
- d'accéder à toute information utile à des fins de diagnostic et d'administration du système, en s'interdisant scrupuleusement de divulguer ces informations.

3.1.2 Transparence des opérations effectuées

Les administrateurs ont le devoir d'informer, dans la mesure du possible, les utilisateurs de toute intervention nécessaire, susceptible de perturber ou d'interrompre l'utilisation habituelle des moyens informatiques.
De même ils s'engagent à informer l'utilisateur de toute opération inhabituelle tendant à accéder à ses données personnelles, directes ou indirectes, sur son poste informatique, et des motifs l'y autorisant conformément à l'exercice de ses missions (sauf au cas où la discrétion des opérations est imposée par les autorités judiciaires).

Tout matériel autre que les postes informatiques (PC, ordinateurs portables, etc.) destiné à être connecté au réseau filaire de l'UBE - tels que les objets connectés, robots, ajout d'équipement manageable et non manageable etc. - doit faire l'objet d'une demande préalable auprès de la DNUM avant tout achat. Cette demande permet de vérifier la compatibilité réseau, l'absence de risque de sécurité, ainsi que la disponibilité d'une prise réseau à l'endroit prévu pour l'installation.

3.1.3 Chaine d'alerte

Les administrateurs ont le devoir d'informer immédiatement leur responsable hiérarchique direct, le CSSI ou les CSSI de leur composante, laboratoire, service... ainsi que le RSSI de l'université (ou son suppléant) de toute tentative d'intrusion sur un système, de toute faille de sécurité détectée, ou de tout comportement d'utilisateur pouvant compromettre la sécurité du système informatique de l'université, dont il aurait eu connaissance pendant l'exercice de ses missions.

Le schéma de la chaine fonctionnelle est disponible via l'ENT ou l'intranet.

3.1.4 Sensibilisation des utilisateurs

Les administrateurs ont le devoir de sensibiliser les utilisateurs :

- rappeler les principes d'usage du réseau RENATER et les différentes chartes de l'UBE relatives aux systèmes d'information à tout utilisateur semblant les méconnaître ;
- informer les utilisateurs des consignes techniques de sécurité à mettre en œuvre afin de préserver le système informatique général et individuel ;
- sensibiliser aux risques juridiques encourus par l'université et eux-mêmes du fait de leur comportement (installation de logiciels sans licence, copies de sauvegarde sans autorisation, usage illégal ou non conforme des ressources informatiques) ;
- inciter les usagers à suivre les formations sur la Sécurité des systèmes d'Information présents au plan de formation UBE.

3.2 Les moyens

3.2.1 Les sauvegardes automatiques

Chaque application génère des fichiers de données informatisées qu'il convient de sauvegarder régulièrement pour assurer la continuité du service informatique en cas de perte ou d'altération de données. Ces données doivent être sauvegardées régulièrement de manière à assurer, dans la mesure du possible et selon les moyens disponibles, toute récupération de données.

3.2.2 La métrologie en temps réel

Un ensemble d'outils de supervision est actif pour l'ensemble du réseau de l'université pour en assurer un fonctionnement optimum. Ils permettent de faire de la métrologie (étude de la charge du réseau). Cette étude permet d'optimiser les ressources et de détecter les anomalies de fonctionnement, permettant ainsi à l'administrateur de procéder à une analyse plus fine en exploitant les « traces » d'opérations informatiques.

3.2.3 La traçabilité des opérations informatiques

Le bon fonctionnement et la sécurité du système informatique nécessitent l'enregistrement systématique et automatique d'un certain nombre d'informations caractérisant chaque opération informatique, appelées « traces ».
Ces traces sont toutes exploitables et peuvent conduire à reconstituer exactement un évènement informatique survenu, permettant ainsi à l'administrateur de réaliser la maintenance du service.

Ces traces ont deux objectifs exclusifs :

- → Assurer le bon fonctionnement des services et déterminer leurs améliorations possibles ;
- → Détecter toute anomalie de sécurité et être à même de mener les enquêtes correspondantes.

Elles sont exploitées sous forme de :

- statistiques non individuelles ;
- analyses par machine des opérations effectuées ;
- recherches manuelles précises sur un type de problème.

Les administrateurs s'engagent à n'utiliser les traces que si un motif légitime les y oblige, conformément aux droits et devoirs que leur confèrent leurs missions.

Article 4. Cadre juridique de l'intervention

« L'informatique ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques » (Article 1er de la loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers, et aux libertés).
Aucune exploitation, à des fins autres que celles liées à leurs missions, des informations dont les administrateurs ont connaissance pendant l'exercice de leurs missions, ne saurait être opérée, d'initiative ou sur ordre hiérarchique, qui aurait pour conséquence de violer les droits et libertés fondamentaux de l'utilisateur, tels que décrits ci-dessous.

Par conséquent, l'administrateur s'engage à respecter les droits fondamentaux des utilisateurs lors de l'exercice de ses missions, et plus particulièrement :

- le droit au respect de la vie privée ;
- le droit au secret des communications électroniques ;
- le droit au secret des correspondances.

Par ailleurs, ils ont le devoir de désobéir à tout ordre qui aurait pour conséquence de leur faire commettre une infraction, que ce soit suite à la violation d'un droit fondamental de l'utilisateur tel que décrit ci-dessus, ou à la loi du 6 juillet 1978 modifiée en août 2004.

Seules les autorités judiciaires, en tant que gardiennes des libertés individuelles, ont la faculté de déroger à ces principes en cas de nécessité liée à la recherche de preuves dans le cadre de l'instruction d'une affaire ou d'une enquête.

4.1 Respect de la loi relative à l'informatique, aux fichiers et aux libertés, RGPD

La loi informatique et liberté pose des définitions ci-dessous énumérées, avant de poser les conditions de licéité d'un traitement de données personnelles, et les règles d'accès aux données personnelles de l'utilisateur sur son poste de travail.

4.2 Définitions / références juridiques

Les principales dispositions légales en vigueur prévues par la législation française sont décrites dans l'annexe juridique associée à la charte de bon usage des moyens numériques de l'université (document principal).

Chaque administrateur devra connaître les définitions de :

- donnée à caractère personnel ;
- conditions de mise en œuvre d'un traitement automatisé de données à caractère personnel.

4.2.1 Les obligations spécifiques de l'administrateur, responsable du fichier

Le responsable d'un traitement de données à caractère personnel est (sauf désignation expresse par les dispositions législatives ou règlementaires relatives à ce traitement) *la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens* ; c'est à lui qu'incombe :

- d'accomplir les formalités préalables à la mise en œuvre du traitement auprès du DPO ;
- d'informer l'utilisateur de l'identité du responsable du fichier, de celles des destinataires des données, des droits d'accès, de rectification et d'opposition dont il dispose ;
- assurer la sécurité des données contre toute altération, modification ou communication à des tiers non autorisés en prenant toute précaution utile ;
- recueillir le consentement préalable des personnes concernées.

4.2.2 Les conditions de collecte des données et de traitement

Ces conditions s'appliquent à tout administrateur chargé de la mise en œuvre du traitement, lequel doit veiller à leur bonne application.

La collecte des données et leur traitement doivent être : « loyaux et licites ».

Pour des « *finalités déterminées, explicites et légitimes* » ;

4.2.3 Précautions particulières lors du traitement de données personnelles

Des précautions particulières s'imposent pour les administrateurs ayant connaissance de données à caractère personnel au cours de leur enregistrement, classement, transmission ou toute autre forme de traitement de données, afin d'éviter :

- toute divulgation, même par imprudence ou négligence ;
- de détourner ces informations de la finalité de leur traitement initial tel que défini par la disposition législative.

4.2.4 Accès aux données personnelles de l'utilisateur sur son poste de travail

L'administrateur s'engage à 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 son cadre d'intervention comme défini ci-après.

Il est recommandé à l'utilisateur de classer ses données dans un répertoire nommé « Privé ».

Accès direct sur les postes (intervention sur site)

En tout état de cause, et lorsque l'intervention le nécessite, l'accès direct aux données enregistrées par les utilisateurs dans leur propre environnement informatique, qui sont parfois de nature personnelle, ne peut être justifié que dans les cas où le bon fonctionnement des systèmes informatiques ne pourrait être assuré par d'autres moyens moins intrusifs, et si l'utilisateur a été informé (ce qui est implicite dès lors qu'il a autorisé l'administrateur à intervenir sur son poste de travail afin de résoudre un problème).

Accès indirect sur les postes (intervention à distance)

Toute personne utilisatrice des réseaux de communications électroniques doit être informée de manière claire et complète par le responsable du traitement ou son représentant :

- De la finalité de toute action tendant à accéder, par voie de transmission électronique, à des informations stockées dans son équipement terminal de connexion, ou à inscrire, par la même voie, des informations dans son équipement terminal de connexion ;
- Des moyens dont elle dispose pour s'y opposer.

4.3 Obligation de confidentialité et secret professionnel

Les administrateurs ayant la qualité de fonctionnaires sont soumis au secret professionnel de par leur statut général.
Les agents non titulaires, sans être astreints au secret professionnel, sont dans la nécessaire confidence concernant les informations dont ils pourraient avoir connaissance pendant l'exercice de leurs missions, et sont soumis, en ce qui concerne les données à caractère personnel dont ils pourraient avoir connaissance durant leur mission, à une obligation de non-divulgation.

L'administrateur a le devoir de transmettre tous les faits constitutifs de délits ou de crimes dont il aurait pu avoir connaissance durant l'exercice de sa mission en suivant la chaine fonctionnelle de sécurité des systèmes d'information.
Ces faits constitutifs d'infractions sont énumérés en annexe, sans être limitatifs aux seuls faits informatiques.

5. Engagements

L'administrateur s'engage à respecter en toute circonstance la législation en vigueur, ainsi que les règles de la PSSIE et de la présente charte ainsi que toutes les chartes régissant l'usage du système d'information.
Pour cela, il est accompagné à travers les dispositifs universitaires d'information et de formation.

En cas de doute ou de question, l'administrateur du système d'information pourra demander conseil auprès :

- **Du fonctionnaire Sécurité Défense**
- **Du service juridique**
- **Du DPO**
- **De la DNUM**

Président de l'Université Bourgogne Europe

Vincent Thomas