



CHARTRE DE BON USAGE DES MOYENS NUMÉRIQUES DE L'UNIVERSITÉ

Administrateur informatique

Valérie GIBERT

Directrice générale des services

Affaire suivie par

Guy BRAND

*Responsable de la sécurité
des systèmes d'information*

Tél. : +33 (0)3 68 85 06 88

gb@unistra.fr

SOMMAIRE

INTRODUCTION	3
ARTICLE 1 : ADMINISTRATEUR	3
ARTICLE 2 : DROITS DE L'ADMINISTRATEUR	3
ARTICLE 3 : DEVOIRS DE L'ADMINISTRATEUR	3
ARTICLE 4 : RÉFÉRENCES JURIDIQUES	4
ARTICLE 5 : ENGAGEMENTS	4

Introduction

La présente charte constitue une annexe du règlement intérieur au même titre que la charte de bon usage des moyens numériques de l'Université de Strasbourg. Elle est librement consultable via l'environnement numérique et social de travail de l'Université de Strasbourg, dénommé Ernest. Elle engage pleinement la responsabilité de l'agent en cas d'infraction, ou de complicité d'infraction, à la réglementation en vigueur et au règlement intérieur de l'université.

Le Comité Technique d'Etablissement (CTE) en a examiné les dispositions lors de sa séance du 10 décembre 2015. La date d'entrée en vigueur est immédiate.

Article 1 : Administrateur

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 réseaux, 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 telles 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 réglementaires régissant son statut, excluant de fait toute utilisation de ses droits d'accès privilégiés à des fins personnelles.

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 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 ponctuellement, sur demande formelle de l'utilisateur lui-même - et n'autorise quiconque à y accéder, sauf cas particuliers 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 réglementation sur la protection des données à caractère personnel ;
- informe le Responsable de la Sécurité des Systèmes d'Information (RSSI) de tout incident de sécurité dont il pourrait avoir connaissance ;
- 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 ;
- agit dans le sens d'une meilleure sécurité, dans l'intérêt de l'établissement et des utilisateurs.

Article 4 : 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 de Strasbourg.

Article 5 : Engagements

L'administrateur s'engage à respecter en toutes circonstances la législation en vigueur et le règlement intérieur de l'université incluant les dispositions de la présente charte.

En cas de non-respect, l'administrateur sera tenu pour responsable de ses actes et pourra encourir des sanctions disciplinaires, civiles ou pénales.

La Directrice générale des services,
Valérie GIBERT