CHARTE DE L'ADMINISTRATEUR DE SYSTÈMES INFORMATIQUES
(v20180118)

La composante informatique du système d'Information (SI) de l'Université de Lille prend une part prépondérante dans celui-ci. En outre, elle s'ouvre à d'autres acteurs que les membres de l'Université.

Parallèlement, le contexte juridique qui encadre les systèmes d'information se complexifie en intégrant continuellement de nouvelles législations et réglementations françaises et européennes.

Cette situation impose à l'établissement de sécuriser les activités des personnes ayant des droits étendus sur les systèmes informatiques et en particulier des administrateurs de systèmes informatiques.

Cette charte de l'administrateur de systèmes informatiques vient en complément du règlement d'usage du système d'information par les utilisateurs de l'Université. Elle vise à présenter les règles de déontologie (sans les limiter) auxquelles l'administrateur de systèmes informatiques doit se conformer.

Ce document s'adresse à tous les administrateurs de systèmes informatiques amenés à intervenir dans le système d'information de l'Université, qu'ils soient agent fonctionnaire ou contractuel de droit public de l'établissement ou des établissements partenaires, salarié des prestataires extérieurs ou stagiaire en formation.

Toutefois, elle ne se substitue pas aux lois en vigueur et ne traite pas des systèmes classifiés Défense.

L'administrateur de systèmes informatiques, dans le cadre de ses activités professionnelles, a pour mission d'assurer le fonctionnement *normal* et *sécurisé* des réseaux, des systèmes, des matériels, des logiciels et des bases de données de l'établissement, délégués à l'établissement ou sous traités pour le compte de l'établissement.

Normal : assurer la finalité pour laquelle l'élément a été conçu dans un cadre légal et professionnel.
Sécurisé : garantir le niveau adéquat de disponibilité, d'intégrité et de confidentialité de l'élément.

« L'administrateur de systèmes informatiques » sera nommé administrateur dans la suite du document.

Les droits d'accès privilégiés

Les activités de déploiement, d'administration, de supervision, d'exploitation et de maintenance informatiques amènent l'administrateur à acquérir des droits d'accès privilégiés aux informations personnelles relatives aux utilisateurs.

L'administrateur, après s'être identifié, use de ces accès privilégiés dans le respect strict de la finalité de ses missions.

Néanmoins, il peut utiliser une identification générique lorsque l'identification personnelle est impossible ou pourrait nuire au bon fonctionnement ou à la sécurité du système informatique.

Il attribue, modifie ou supprime les accès privilégiés des utilisateurs dans un cadre de procédures définies par l'établissement.

L’accès aux données personnelles des utilisateurs gérées par l’établissement

L’accès aux données enregistrées par les utilisateurs dans l’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.

De même, l’administrateur ne doit pas divulguer des informations qu’il aurait été amené à connaître dans le cadre de ses fonctions, et en particulier lorsque celles-ci sont couvertes par le secret des correspondances ou relèvent de la vie privée des utilisateurs et ne mettent en cause ni le bon fonctionnement technique des applications, ni leur sécurité, ni l’intérêt de l’établissement. Il ne saurait non plus être contraint de le faire, sauf disposition législative particulière en ce sens.

L’administrateur est tenu à une obligation de confidentialité.

L’utilisation des logiciels de prise de main à distance

Les logiciels de prise de main à distance peuvent notamment permettre à l’administrateur d’accéder à distance à l’ensemble des données de n’importe quel poste de travail, à des fins de maintenance informatique.

Les actions de télémaintenance ne peuvent pas être détournées pour contrôler ou surveiller l’activité des utilisateurs sur leur poste de travail.

L’administrateur doit s’entourer de précautions pour garantir la transparence dans l’emploi des logiciels de prise de main à distance et la confidentialité des données auxquelles il accède par ce moyen dans la stricte limite de ses besoins.

Doivent a minima figurer au titre de ces précautions :

- l’information préalable et le recueil de l’accord de l’utilisateur pour « donner la main » à l’administrateur avant l’intervention sur son poste;
- la traçabilité des opérations de maintenance par la tenue d’un registre des interventions.

La gestion des traces informatiques

L’administrateur met en œuvre la gestion des traces informatiques à l’aide de mécanismes de journalisation pour suivre le bon fonctionnement et la sécurité du système informatique.

Il accède aux journaux informatiques dans le seul but de diagnostiquer les dysfonctionnements ou les incidents de sécurité qui touchent ces systèmes.

Il garantit l’intégrité, la disponibilité et la confidentialité de ces journaux jusqu’à leur date légale de destruction.

L’arrêt des mécanismes de journalisation est autorisé, après que le responsable de la sécurité du système d’information ait été informé, à seule fin d’éviter la saturation des capacités du système informatique.

La continuité de service

L'absence de l'administrateur ne doit pas perturber le fonctionnement de l'établissement. Il est important que celui-ci documente les éléments essentiels de ses activités de développement, de déploiement, d'administration, de supervision, de maintenance et celles qui sont connexes (procédures, configurations, projets).

Il s'assure que les données d'identification et d'authentification des comptes génériques d'administration sont accessibles par la direction de l'établissement.

Il informe sa hiérarchie des dispositions qu'il a prises à propos de ses activités avant la fin de son affectation au sein de l'établissement.

L'information et l'alerte

L'administrateur peut être amené à mettre en œuvre des traitements sur des données à caractère personnel.

Il s'assure auprès du correspondant informatique et libertés que ces traitements soient déclarés.

L'administrateur veille à ce que les traitements et les données qui sont utilisés ou stockés dans le système informatique de l'établissement ne portent pas atteinte à la propriété intellectuelle et au droit des tiers.

Il informe son responsable hiérarchique et le responsable de la sécurité du système d'information de toute infraction dont il a connaissance.

L'administrateur alerte le responsable de la sécurité et son responsable hiérarchique des failles et des incidents de sécurité dont il pourrait avoir connaissance.

L'administrateur est régulièrement amené à programmer un arrêt du système informatique pour des raisons de maintenance ou de mise à niveau.

Il informe suffisamment à l'avance son responsable hiérarchique, le dépositaire du système concerné, le responsable de la sécurité du système d'information et le cas échéant les utilisateurs de son intention d'arrêter le système informatique.

Il alerte le responsable de la sécurité du système d'information sur les demandes d'accès aux informations ou de divulgation d'information à titre d'autorité judiciaire dont il pourrait être assujetti.