

**Nom du client**

**Charte de sécurité des administrateurs informatiques**

Informations générales

Version : 0.7

État : Draft

Projet : Charte de sécurité des Administrateurs informatiques

Mise en vigueur : 11/12/2019

Représentant :

# Objet de la charte

L’administrateur informatique est une personne clé qui doit posséder des privilèges particuliers pour assurer ses fonctions au sein du système d’information. À ce titre, son professionnalisme et sa rigueur sont primordiaux. La charte définit devoirs de l’administrateur dans le cadre de ses fonctions.

# Définition

Le terme « Administrateur informatique » désigne toute personne, quelle que soit sa fonction, qui a pour rôle et missions d’assurer le bon fonctionnement et la sécurité des ressources des systèmes d’informations placés sous sa responsabilité (tels que les serveurs, les équipements réseau, les équipements de sécurité, les applications, les bases de données, les postes de travail utilisateurs, etc.)

Dans la suite du document, l’administrateur informatique sera désigné par le terme administrateur.

# Devoirs de l’administrateur

L’administrateur est soumis à une obligation de confidentialité liée à ses activités, dans ce cadre :

* Il n’abuse pas de son statut ou des privilèges associés à sa fonction pour avoir accès à des informations ne lui étant pas directement destinées, ou non nécessaires à l’exécution de ses fonctions.
* Il ne donne accès aux informations du système à un tiers que dans le cadre de ses fonctions et/ou sur demande explicite de sa hiérarchie dans le cadre de procédures formalisées ou dans les cas particuliers prévus par la loi.
* Il n’abuse pas de son statut ou des privilèges associés à sa fonction pour avoir accès à des données personnelles d’utilisateurs, sauf, ponctuellement, sur demande de l’utilisateur lui-même, et n’autorise quiconque à y accéder, sauf cas particulier prévus par la loi (par exemple, sur requête du parquet dans le cadre d’une enquête judiciaire) ou habilitation formelle et légitime préalablement déclarée.
* Il n’abuse pas de son statut ou des privilèges associés à sa fonction pour avoir accès à des contenus marqués comme « privés » sauf en présence de l’utilisateur ou avec son autorisation.
* Il respecte les engagements de confidentialité associés à sa fonction ou tout contrat spécifique en rapport signé par lui ou son organisation. Il ne fait pas état et n’utilise pas les informations confidentielles qu’il peut être amené à connaître dans le cadre de ses fonctions, pendant son contrat et après la fin de ce dernier.
* Il ne se connecte pas ou ne donne pas l’ordre à un tiers d’accéder à une ressource du SI sans autorisation de la personne à qui elle est attribuée, notamment dans le cas de l’utilisation d’un logiciel de prise de main à distance sur un poste de travail utilisateur.

Par ailleurs:

* Il documente ses actions et interventions de telle sorte qu’il ne soit pas dans un état de dépendance lors d’un départ.
* Il lui appartient de faire remonter à son supérieur hiérarchique, des informations relatives à la sécurité.
* Il ne prend aucune initiative qui pourrait nuire aux intérêts de la société et agit de bonne foi en toute circonstance.

De plus, l’administrateur observe strictement les règles de sécurité et les limites fixées à ses interventions :

* Il n’abuse pas de ses privilèges, et limite ses actions aux ressources informatiques dont il a la charge, dans le respect de la finalité de sa mission. En particulier, il ne modifie les configurations et les droits d’accès que dans le respect de procédures d’administration ou d’exploitation définies.
* Il ne prend pas ses consignes d’une personne non identifiée et fait remonter auprès de son responsable hiérarchique toute requête lui paraissant inappropriée.
* Il ne contourne pas les procédures de sécurité établies, et en particulier ne désactivent pas de sa propre initiative les mécanismes de traçabilité, et ne portent pas atteinte à l’intégrité des fichiers de journalisation.
* Il n’utilise les comptes privilégiés que pour les activités et besoins directement liés aux tâches d’administration ou d’exploitation dont il a la charge, étant donné que toute action sur les systèmes d’information peut faire l’objet d’une journalisation permettant leur imputabilité.

Dans le cas où un incident de sécurité se produit :

* Il informe son responsable hiérarchique et selon le cas, le responsable de la sécurité des systèmes d’information de son entité - de toute faille ou tout incident de sécurité qu’il pourrait découvrir ou dont il pourrait avoir connaissance.
* Il préserve, conserve et sauvegarde les « traces » nécessaires à la résolution d’un incident et à toute investigation ultérieure.

Enfin, l’administrateur s’assure de la protection des droits d’accès liés à sa fonction :

* Il observe les règles de sécurité en vigueur visant à protéger l'utilisation des comptes et des privilèges qui lui ont été attribués.
* Il veille à la protection des postes de travail à partir desquels il exerce ses fonctions et à la gestion des identifiants et authentifiant des comptes privilégier.
* Les paramètres d’authentification utilisés pour les opérations d’administration doivent être robustes et gérés selon les bonnes pratiques. Ils sont personnels et incessibles.

# Respect de la législation et de la présente charte

L’administrateur informatique s’engage à respecter en toutes circonstances la législation en vigueur auxquels s’ajoutent les règles de la présente charte.

En cas de non-respect de la législation en vigueur et des dispositions de la présente charte, l’administrateur informatique sera tenu responsable de ses actes et pourra encourir des sanctions, ainsi que toute autre sanction civile ou pénale prévue par la loi.

Ce document est une aide à la création d’une charte de sécurité des administrateurs informatiques. Il reprend les grandes lignes des bonnes pratiques et consignes devant être respectées par les administrateurs concernés. Les informations contenues dans ce document ne sont pas exhaustives et devrons toujours être personnalisées à l’organisme receveur, sachant qu’une bonne pratique peut être acceptée, adaptée ou même rejetée selon le contexte.

La présente charte ne substitue en aucun cas l’application éventuelle d’autres chartes auxquels les administrateurs pourront être soumis.

Ni NC3, ni un de ses représentants, ne pourront être tenus responsable de l’usage et des conséquences résultant de ce texte.

**À SUPPRIMER lors de la mise en contexte de la charte**