



## Charte de l'administrateur des systèmes d'information

## SOMMAIRE

1.	OBJET	3
2.	REFERENTIEL	3
3.	DEFINITIONS	3
4.	CHAMP D'APPLICATION	3
5.	PREROGATIVES DE L'ADMINISTRATEUR DES SYSTEMES D'INFORMATION	4
5.1.	Administration des systèmes d'information	4
5.2.	Participation à la politique de sécurité	4
5.3.	Gestion des risques et des menaces	4
6.	ENGAGEMENTS DE L'ADMINISTRATEUR DES SYSTEMES D'INFORMATION	6
6.1.	Obligation de collaboration	6
6.2.	Obligation d'information, de conseil et d'alerte	6
6.3.	Obligation de confidentialité renforcée	6
6.4.	Obligation de sécurité	6
6.5.	Obligation de respecter les droits de propriété	7
6.6.	Obligation de respecter la vie privée des utilisateurs	7
6.7.	Obligation de respecter la réglementation Informatique et libertés	7
7.	RESPONSABILITE	7
8.	ÉVOLUTION DE LA CHARTE	8
9.	ACCEPTATION DE LA CHARTE	8

## 1. OBJET

---

La présente charte a pour objet de définir les principales prérogatives, les engagements et la responsabilité des administrateurs des systèmes d'information d'IFPEN, ci-après appelés « administrateurs » dans la limite de leurs périmètres de responsabilité et conformément aux engagements contractuels dans le cas de prestataires.

## 2. REFERENTIEL

---

La présente charte prend place au sein d'un référentiel qui se compose des documents suivants :

- la présente charte de l'administrateur des systèmes d'information ;
- la charte des systèmes d'information ;
- le livret utilisateur de la charte des systèmes d'information.

## 3. DEFINITIONS

---

Les termes définis dans la charte des systèmes d'information de l'entreprise s'appliquent à la présente charte. Les termes complémentaires relatifs à la charte de l'administrateur sont définis dans ce chapitre.

Au sens de la présente charte, les termes ci-dessous ont la signification suivante :

- « Administrateur d'application » : personne en charge de gérer et administrer la configuration de solutions logicielles développées en interne ou de solutions progiciels disponibles sur étagère.
- « Administrateur de bases de données » : personne en charge de gérer et administrer les systèmes de gestion des données de l'entreprise et d'en assurer la cohérence, la qualité et la sécurité.
- « Administrateur système, réseau et sécurité » : personne en charge de gérer et administrer les logiciels systèmes et/ou les infrastructures de communication (réseau local, étendu, voix, image, architecture centralisée, client-serveur, web, mobile) et/ou les infrastructures de sécurité informatique.
- « Autorité de référence » : personne dont l'emploi ou la fonction lui confère une autorité sur l'administrateur des systèmes d'information. Suivant les cas, il s'agira soit du responsable hiérarchique du salarié, soit du donneur d'ordres dans le cas d'une sous-traitance de l'administration.

## 4. CHAMP D'APPLICATION

---

La présente charte s'applique à tout salarié ou sous-traitant dont la fonction lui confère des droits d'administration sur l'ensemble ou un sous-ensemble des systèmes d'information. Elle ne se substitue pas à la charte des systèmes d'information d'IFPEN qui s'applique à tous les utilisateurs.

Cette charte s'applique quelle que soit l'étendue des droits d'administration conférés, qu'il s'agisse :

- des administrateurs internes ou externes, techniques et/ou fonctionnels (administrateur système, réseau et sécurité, administrateur de bases de données, administrateur d'application) ;
- de toute autre personne qui de par sa fonction dispose d'un droit d'administration sur une quelconque partie des systèmes d'information d'IFPEN, d'applications ou d'équipements informatiques.

Dans le cas d'un administrateur externe (ou prestataire), cette charte s'applique uniquement et exclusivement aux périmètres définis à son contrat. Les actions réalisées par celui-ci sont placées sous l'autorité et le contrôle du donneur d'ordres.

## 5. PREROGATIVES DE L'ADMINISTRATEUR DES SYSTEMES D'INFORMATION

---

### 5.1. ADMINISTRATION DES SYSTEMES D'INFORMATION

L'administrateur assure le bon fonctionnement général des systèmes d'information dont il a la charge, notamment en ce qui concerne leur performance, leur disponibilité et leur interopérabilité.

Il maintient le bon état de fonctionnement des outils dont il a la charge.

Il paramètre et analyse les fichiers d'historisation pour identifier le cas échéant des dysfonctionnements ou des fonctionnements anormaux.

Il met en œuvre, en tant que de besoin, les profils utilisateurs conformément aux exigences définies par la Direction du système d'information d'IFPEN.

Lorsqu'il procède à des interventions à distance sur l'outil d'un utilisateur, l'administrateur devra requérir la présence de l'utilisateur, ou à tout le moins avoir un accord écrit au préalable de l'utilisateur ou à défaut de son donneur d'ordres.

L'administrateur participe activement aux mesures de sauvegarde mises en œuvre par IFPEN selon son périmètre de responsabilité.

À ce titre, les cas de non-respect par des utilisateurs des dispositions contenues dans la charte des systèmes d'information d'IFPEN et/ou dans le livret utilisateur de la charte devront être signalés à la Direction du système d'information.

### 5.2. PARTICIPATION A LA POLITIQUE DE SECURITE

L'administrateur doit prendre toutes les mesures appropriées permettant d'attester du respect de la législation applicable en matière de la protection des données et de leurs traitements.

Dans le cas d'une administration réalisée dans le cadre d'un contrat de prestation, l'administrateur prendra les mesures relevant de la responsabilité du sous-traitant au sens du RGPD (Règlement général pour la protection des données à caractère personnel).

L'administrateur devra se conformer à la politique de sécurité des systèmes d'information d'IFPEN et contribuer à sa mise en œuvre dans la limite de ses périmètres de responsabilité.

L'administrateur pourra, sur demande de l'autorité de référence, procéder à un audit interne de tout ou partie des systèmes d'information d'IFPEN, et ce conformément au cadre des engagements définis au contrat dans le cas des prestataires.

### 5.3. GESTION DES RISQUES ET DES MENACES

En fonction des prérogatives qui lui sont attribuées, l'administrateur prend part aux opérations de maintenance du système d'information d'IFPEN. Dans ce cadre, il procède à la correction de toute anomalie du système d'information, préconise et met en place des solutions de contournement

permettant d'assurer la continuité des services. Actions qui devront être réalisées après accord de l'autorité de référence, conformément au cadre des engagements définis au contrat dans le cas des prestataires.

À ce titre, l'administrateur utilise tous les moyens de sécurité mis à sa disposition pour procéder à cette maintenance et met notamment en place les patches de sécurité nécessaires au maintien en condition de sécurité du système d'information. Actions qui devront être réalisées après accord de l'autorité de référence, conformément au cadre des engagements définis au contrat dans le cas des prestataires.

Il peut, à cette occasion, identifier des comportements anormaux de la part des utilisateurs.

Dans tous les cas où il aura constaté un dysfonctionnement ou un usage anormal du système d'information, il en informe immédiatement la Direction du système d'information.

L'administrateur ne procédera à un approfondissement d'alerte qu'après que son autorité de référence lui ait accordé le droit de faire une analyse approfondie des dysfonctionnements qui auraient fait l'objet d'une alerte auprès d'elle.

Dans cette hypothèse, il met en œuvre les mesures prescrites par cette autorité.

En cas de force majeure ou de mesures d'urgence, l'administrateur peut intervenir seul et prendre les mesures nécessaires au maintien de la sécurité, de l'intégrité, de la disponibilité, de la confidentialité et du bon fonctionnement du système d'information.

Dans ce cas, il informe immédiatement son autorité de référence des actions qu'il met en œuvre et de leurs conséquences et des solutions alternatives adoptées visant au maintien du bon fonctionnement des systèmes d'information d'IFPEN.

En cas de présomption de violation par un utilisateur de la charte des systèmes d'information d'IFPEN, basée sur des indices, l'administrateur pourra prendre le contrôle du poste de l'utilisateur avec ses propres identifiants pour protéger le système d'information ou éviter la propagation de codes malveillants.

En cas d'absence d'un utilisateur et pour assurer la continuité du service, l'administrateur peut, sur demande du management (directeur ou chef de département) de la Direction compétente (Direction de l'utilisateur, Direction du système d'information, Direction des ressources humaines) prendre le contrôle du poste de l'utilisateur et communiquer ou router les fichiers, les mails ou les documents professionnels (à l'exclusion donc des données identifiées comme personnels) auprès de toute personne qui lui aura été désignée.

L'administrateur qui aurait identifié un contenu propageant un code malveillant ou susceptible de l'être est en droit de prendre toutes mesures appropriées de nature à bloquer la propagation dudit code.

En cas d'incident de sécurité avéré tel que tentative d'intrusion, attaque virale, usurpation d'identité, vol de matériel ou d'information, cette liste n'étant pas exhaustive, les actions de correction sont pilotées par la Direction du système d'information d'IFPEN en concertation avec la sécurité et les responsables concernés.

### 6.1. OBLIGATION DE COLLABORATION

L'administrateur coopère étroitement dans le cadre de l'exécution de ses obligations avec son autorité de référence. À cette fin, il procède à un échange permanent d'informations en vue de contribuer à la bonne exécution de ses obligations et au fonctionnement des systèmes d'information.

### 6.2. OBLIGATION D'INFORMATION, DE CONSEIL ET D'ALERTE

L'administrateur s'engage à une obligation générale d'information, de conseil, d'alerte et de mise en garde auprès de son autorité de référence.

L'administrateur assure une veille générale des systèmes d'information d'IFPEN et informe son autorité de référence de tout dysfonctionnement qu'il pourrait constater.

### 6.3. OBLIGATION DE CONFIDENTIALITE RENFORCEE

L'administrateur s'engage à respecter une confidentialité absolue sur l'ensemble des données, fichiers, traitements et informations dont il pourrait avoir connaissance.

L'administrateur s'engage à garder confidentielles et à ne pas divulguer à des tiers toutes informations qui lui ont été révélées et dont il a eu connaissance.

L'administrateur s'engage à ne pas faire, directement ou indirectement, un usage desdites informations autre que celui nécessaire à la réalisation des missions dont il a la charge.

L'administrateur s'engage à prendre toutes les mesures de sécurité nécessaires à la protection des informations et au maintien de leur confidentialité absolue.

L'administrateur s'engage à respecter la plus stricte confidentialité des mots de passe des utilisateurs et à garder strictement confidentiel les mots de passe des comptes d'administration, à ne les dévoiler à personne, ni les écrire, ni les enregistrer sur un support quelconque pour la mémorisation sauf à utiliser les outils spécialisés et sécurisés (type coffre-fort de mots de passe) mis à disposition par la Direction du système d'information d'IFPEN, à l'exclusion de tout autre.

L'administrateur s'interdit de porter atteinte, sous quelque forme que ce soit et pour quelque motif que ce soit, au secret des correspondances (courrier électronique, SMS, messagerie instantanée, ...).

### 6.4. OBLIGATION DE SECURITE

L'administrateur s'engage à n'utiliser que les moyens informatiques et de communications électroniques confiés et/ou validés par la Direction du système d'information d'IFPEN et s'interdit d'utiliser toute autre solution notamment dans le cadre d'opérations de contrôle ou d'audit.

L'administrateur s'engage à documenter toute action et intervention en écart avec les procédures internes d'IFPEN.

L'administrateur s'engage à ne pas porter atteinte à l'intégrité des fichiers de journalisation.

L'administrateur s'engage à remonter sans délai toute information relative à toute faille ou incident de sécurité qu'il pourrait découvrir ou dont il pourrait avoir connaissance.

L'administrateur s'engage à n'utiliser les comptes d'administration que pour les activités et besoins directement liés aux tâches d'administration ou d'exploitation dont il a la charge. L'administrateur doit utiliser un compte non privilégié lorsqu'il effectue des actions plus exposées, comme lire ses courriels ou naviguer sur internet.

L'administrateur s'engage à ne prendre aucune consigne d'une personne non identifiée et, le cas échéant, à transmettre à son autorité de référence toute requête lui paraissant inappropriée.

## **6.5. OBLIGATION DE RESPECTER LES DROITS DE PROPRIETE**

Dans le cadre de l'exercice de ses missions, l'administrateur s'engage à ne pas porter atteinte à des droits de propriété intellectuelle.

Il s'engage notamment à :

- ne pas installer et ne pas utiliser sur les matériels informatiques d'IFPEN un logiciel et/ou un progiciel sans qu'une licence d'utilisation appropriée n'ait été préalablement souscrite ;
- ne pas pratiquer des téléchargements illicites, notamment dans le cadre du téléchargement de logiciels ou de bases de données sécuritaires ;
- ne pas reproduire ou utiliser des créations protégées par le droit de la propriété intellectuelle sans autorisation ;
- maintenir les formules de copyright.

## **6.6. OBLIGATION DE RESPECTER LA VIE PRIVEE DES UTILISATEURS**

L'administrateur s'engage à respecter la vie privée des utilisateurs qui disposent notamment d'un droit à une vie privée résiduelle relatif à l'utilisation des systèmes d'information d'IFPEN.

Concernant les dossiers, fichiers, données et messages des utilisateurs identifiés comme « perso » susceptibles d'être contenus dans tout ou partie des systèmes d'information, l'administrateur qui serait amené à y accéder s'engage à en assurer la confidentialité et l'intégrité.

## **6.7. OBLIGATION DE RESPECTER LA REGLEMENTATION INFORMATIQUE ET LIBERTES**

L'administrateur s'engage à ne pas procéder à la création de fichiers de données à caractère personnel au sens des dispositions de la loi Informatique et libertés et de la réglementation européenne pour la protection des données personnelles (RGPD) autre que ce qui serait strictement nécessaire à l'accomplissement de sa mission.

Il s'engage en outre au respect de la sécurité, de la finalité et de la confidentialité des données à caractère personnel figurant dans les fichiers appartenant à l'IFPEN.

## **7. RESPONSABILITE**

---

Les moyens mis à la disposition de l'administrateur en sa qualité le sont à des fins exclusivement professionnelles.

L'administrateur s'engage à assurer sa mission dans les limites de la présente charte et de son contrat de travail ou le contrat de prestation de service qui lie son employeur à IFPEN.

A défaut du respect des obligations lui incombant dans le cadre de sa mission ou dans le cas de dépassement non justifié de ses prérogatives, l'administrateur engage sa responsabilité.

Le non-respect de tout ou partie des règles définies dans la présente charte pourra entraîner pour l'administrateur la suppression immédiate du droit d'utilisation des systèmes d'information et, le cas échéant, des sanctions disciplinaires et/ou des poursuites judiciaires.

## 8. ÉVOLUTION DE LA CHARTE

---

Chaque personne destinataire de la présente charte est invitée à transmettre à la Direction du système d'information toute proposition de modification ou d'ajout dont il a pu constater l'intérêt dans le cadre de ses missions d'administrateur ou dans l'exercice de ses fonctions.

La présente charte sera régulièrement mise à jour et sera portée à la connaissance de toute personne concernée sur support papier ou électronique.

## 9. ACCEPTATION DE LA CHARTE

---

Tout administrateur s'engage à respecter la présente charte lors de tout accès au système d'information d'IFPEN.