CHARTE D'ADMINISTRATION

V 0.9.3

SODIAAL

Coopérative Laitière Française

2021

I. Introduction

1. Préambule

Cette charte vient en complément de la Charte utilisateur et s'applique à l'ensemble des utilisateurs du groupe et plus spécifiquement à ceux disposant du statut d'administrateur.

L'administrateur est une personne, **employée ou non par Sodiaal** ; en charge du bon fonctionnement du SI. Il est responsable de son périmètre d'activité où il va mener différentes actions rendues possibles grâce à des droits spécifiques dits « à privilèges ».

Les différents administrateurs sont :

- Administrateur de système
- Administrateur de réseau
- Administrateur de base de données
- Administrateur d'application (Cloud, On Premise)
- Administrateur d'éléments d'infrastructure
- Administrateur des outils collaboratifs (Teams, Intranet, etc.)

En complément chaque utilisateur disposant des **droits à privilège/administrateur sur son poste de travail** est administrateur et doit appliquer la présente politique.

La présente charte a pour objectifs :

- De préciser les **droits et devoirs de l'Administrateur** dans l'exercice de sa fonction ou de son activité professionnelle.
- De permettre **d'éviter toute forme d'abus de l'usage des outils informatiques** et constitue un document **opposable de référence** au sein de Sodiaal.

Cette charte est composée d'un ensemble d'informations **(I)**, de mesures obligatoires **(O)** et de restrictions **(R)** s'appliquant suivant le champ d'application :

2. Champ d'application

La présente charte s'adresse à tout administrateur sur tout ou une partie du SI Sodiaal et ceci qu'il soit :

- Interne ou externe : Collaborateur, Stagiaire, Intérimaire, Prestataire, Alternant
- Temporaire ou permanent : CDD, CDI, Contrat de prestation

La présente charte s'adresse non seulement aux administrateurs, mais également à tout responsable hiérarchique et/ou opérationnel qui a le devoir de faire connaître et respecter la charte par ses équipes dans l'exécution des missions d'administration confiées.

II. Les droits des administrateurs

1. Utilisateurs aux droits étendus

O1	Afin de mener à bien les actions de son périmètre, l'administrateur dispose d'un compte avec des droits à privilèges. Ce compte dispose des caractéristiques suivantes : • Identification du compte comme étant à privilèges (compte nominatif) • Traçabilité des actions effectuées. À ce titre ce compte pourra nécessiter des mesures d'authentification renforcées par rapport aux comptes utilisateurs standards.
R1	Les droits administrateurs ne pourront pas être positionnés sur des comptes génériques ou partagés.
I1	L'administrateur SI peut en particulier effectuer les tâches suivantes : • Isoler, arrêter ou reconfigurer des comptes utilisateurs, des équipements ou des applications informatiques pouvant compromettre la sécurité de l'ensemble du SI de Sodiaal ; • Procéder à des vérifications techniques sur des fichiers de bases de données, de journalisation ou de configuration, afin de déceler tout anomalie ou incident de sécurité qui pourrait porter atteinte au bon fonctionnement du SI de Sodiaal ; • Traiter (détection, analyse, éradication, filtrage, etc.) tout flux informatique présentant des risques potentiels de sécurité (virus, intrusion, utilisation d'un logiciel interdit, etc.).
I2	En cas de comportements anormaux identifiés ou de soupçons sur la légitimité des actions en lien avec l'activité des utilisateurs de Sodiaal, les administrateurs peuvent être amenés à réaliser les actions suivantes moyennant l'information du management et/ou des utilisateurs en respectant l'organisation en place : • Interruption prolongée de service ; • Interruption de toute tâche utilisateur dans le cas où une utilisation excessive des ressources nuit au bon fonctionnement du système (avec ou sans préavis, selon l'urgence du problème) ; • Mise sur un support externe ou compression des fichiers excessivement volumineux ou sans lien direct avec l'activité professionnelle (avec ou sans préavis) en cas de dégradation de service ; • Interruption des sessions de travail trop longtemps inactives. • Blocage temporaire d'un compte et révocation temporaire d'accès

R2	L'utilisation du compte administrateur pour mener des actions quotidiennes sur le SI (consultation d'e-mail, navigation Internet, bureautique, etc.) est interdite. Pour ces actions l'administrateur dispose d'un compte standard. En complément de celui-ci, il dispose de son compte administrateur dédié aux actions d'administration.

2. Utilisation de logiciels et matériels spécifiques

I3	Les administrateurs SI identifiés par Sodiaal peuvent être amenés à utiliser des logiciels particuliers non autorisés aux utilisateurs du SI de Sodiaal, notamment des logiciels permettant d'effectuer des scans sur le réseau ou sur un poste du groupe.
O2	L'utilisation de logiciels de télémaintenance permettant de prendre le contrôle, à distance, du poste de travail d'un utilisateur nécessite l'accord systématique de ce dernier.
O3	L'installation ou la mise à jour de composants sur le SI doit suivre les obligations suivantes : • Uniquement depuis les sources officielles de l'éditeur du logiciel ; • Après vérification de l'intégrité des binaires installés grâce à la cryptographie (Signature numérique des fichiers basée sur un hash : SHA2, SHA256, SHA1, etc.).

III. Les devoirs des administrateurs

1. Généralités

O4	L'administrateur doit se conformer à : • Charte utilisateur • Charte SI (notamment en cas d'installation d'outil sur le poste de travail) • Politiques/procédures existantes • Lois/réglementations applicables • Accords de confidentialité/non divulgation
O5	Tout administrateur doit garder strictement confidentiels les authentifiants de ses comptes personnels, ainsi que des comptes techniques dont il a connaissance dans l'exercice de sa mission.
O6	Les administrateurs doivent s'assurer de l'approbation préalable du propriétaire d'une application ou d'une information avant d'attribuer un droit d'accès à un utilisateur.
O7	Les sessions et outils d'administrations doivent être fermés dès lors que les actions d'administration sont réalisées.

O8	L'administrateur a la charge de l'implémentation des habilitations donnant accès aux données confidentielles. Ces habilitations devront être conformes au principe de droit d'en connaître.
R3	L'administrateur ne doit pas prendre ses consignes d'une personne non autorisée. Il doit informer son responsable hiérarchique de toute demande non légitime. Sa hiérarchie pourra l'autoriser à réaliser ce traitement. L'administrateur ne doit pas mettre en œuvre les demandes lui paraissant contraire la présente charte, aux bonnes pratiques en termes d'hygiène et de sécurité informatique, ou aux lois en vigueur, mais en référer à sa hiérarchie et au responsable de la sécurité du SI de Sodiaal.
R4	L'administrateur ne doit pas contourner les procédures de sécurité établie, et en particulier, il ne doit pas : • Désactiver de sa propre initiative les mécanismes d'authentification et de traçabilité • Porter atteinte à l'intégrité des fichiers de journalisation.
R5	L'administrateur ne doit pas abuser de ses privilèges et doit limiter ses actions aux ressources informatiques dont il a la charge, dans le respect de la finalité de sa mission. En particulier l'administrateur ne doit pas : • Utiliser les actifs de manière détournée, pour un usage personnel • S'octroyer des droits supplémentaires sur le SI.
O9	L'administrateur doit respecter ses engagements de discrétion — confidentialité. À ce titre, il ne doit pas utiliser les informations qu'il peut être amené à connaître dans le cadre de ses fonctions en dehors du groupe.

2. Gestion des incidents

O10	Dans le cas où un incident se produit, l'administrateur informe son responsable hiérarchique et suit le processus de gestion des incidents établi.
O11	Dans le cas où l'incident remet en cause d'une manière ou d'une autre la sécurité du groupe, l'administrateur veillera à conserver l'ensemble des « traces » nécessaires à la résolution de l'incident et à toute investigation ultérieure, et en informera le RSSI Sodiaal.
O12	L'administrateur est soumis à un devoir d'alerte. Dans le cas où un administrateur détecte un évènement, une action, ou un comportement contraire à la charte utilisateur, à la présente charte, ou aux bonnes pratiques en termes d'hygiène et de sécurité informatique il est dans l'obligation d'en alerter sa hiérarchie et le RSSI.
R6	L'administrateur est soumis à un devoir de réserve et ne pourra communiquer ni en interne ni en externe sur un incident dont il aurait connaissance, en dehors des échanges avec les personnes impactées. Sont considérées impactées les équipes de résolution et les personnes notifiées.

O13	Le devoir de réserve de l'administrateur doit être présent dans son contrat de travail ou de prestation.
I4	Les copies effectuées dans le cadre de procédures judiciaires devront respecter le cadre légal applicable : copie à valeur probante, conservation selon les durées nécessaires.

3. La manipulation des données

O14	S'il advient que l'administrateur vienne à connaître le mot de passe associé à un identifiant utilisateur (par exemple dans la cadre d'une réinitialisation), l'administrateur doit rappeler à l'utilisateur son devoir de changer le mot de passe.
R7	L'administrateur ne doit prendre connaissance que des informations pour lesquelles il dispose du besoin d'en connaître, ou sur dérogation formelle de son responsable hiérarchique sous couvert du respect de la règle O6.
R8	L'administrateur n'est pas autorisé à prendre connaissance des données personnelles d'utilisateurs (dont l'identifiant et le mot de passe), sauf cas particulier prévus par la loi (par exemple, commissions rogatoires, enquêtes judiciaires).
R9	L'administrateur n'est pas autorisé à extraire ou copier toute donnée issue du système d'information en dehors du strict exercice de sa mission. Toute extraction ou copie qui serait rendue nécessaire pour concourir au diagnostic d'un incident doit être effacée sous la responsabilité de l'administrateur et dans l'échéance maximale de la résolution de l'incident.
R10	La copie de données de Sodiaal sur un équipement appartenant à un tiers est interdite.
O15	Avant de transférer des données en dehors du groupe, l'administrateur doit vérifier que les destinataires, outils et procédures utilisés sont adaptés à la confidentialité supposée des données.

IV. Contrôle

O16	Toute opération impactant le périmètre de la sécurité (SI, application, infrastructure, etc.) doit obligatoirement donner lieu à un enregistrement (suivi, traces). L'administrateur a donc en charge de la traçabilité de ses actions notamment l'ouverture, le suivi, la documentation des tickets, des mises en production et de tout changement sur son périmètre d'activité.
O17	Il est de la responsabilité des administrateurs d'établir et transmettre les rapports d'incidents, signalant tout évènement mettant en cause la qualité et la sécurité des ressources informatiques du SI de Sodiaal. Il est aussi responsable du signalement de toute infraction à la présente charte et à la charte d'utilisation des ressources informatiques.
I5	Sodiaal se réserve la possibilité de vérifier, de manière automatique ou par des contrôles manuels, la conformité des habilitations en place et des accès effectués. Ces contrôles pourront également cibler la robustesse des mots de passe utilisés.

V. Sanctions applicables

R11	Le non-respect ou la violation des règles et obligations de la présente charte engage la responsabilité de l'administrateur et constituera une faute susceptible de sanctions disciplinaires, telles que décrites par le processus défini dans le règlement intérieur et dans la charte d'utilisation des ressources informatiques.
R12	Par ailleurs, Sodiaal pourra être amenée à communiquer aux autorités compétentes les actes délictueux commis par les administrateurs (par exemple : une activité illicite sur Internet). De même, dans le cadre d'une procédure judiciaire, les autorités compétentes peuvent être amenées à prendre connaissance notamment des fichiers de journalisation. En outre la responsabilité personnelle de l'administrateur pourra être recherchée dans le cas : • De dommages causés à un tiers ou à Sodiaal ; • D'infractions pénales commises au sein du groupe ou au moyen des ressources mises à sa disposition.
R13	Lorsque l'administrateur en cause est un intervenant externe ou tout utilisateur d'un prestataire ou d'un sous-traitant, le non-respect de la charte par l'administrateur pourrait faire l'objet d'une expulsion de ce dernier des locaux et du retrait immédiat de ses droits d'accès.

VI. Glossaire

Mots	Définitions
SI	Système d'Information
RSSI	Responsable de la sécurité des systèmes d'information
Incidents de sécurité	Un incident de sécurité est un évènement non planifié portant atteinte à l'intégrité ou la confidentialité des données du SI, ou portant atteinte à l'image de Sodiaal
Administrateur	L'administrateur est une personne responsable du bon fonctionnement du SI. Il est responsable de son périmètre d'activité où il va mener différentes actions rendues possibles grâce à des droits spécifiques dits « à privilèges » ou droit administrateur.
Authentification	Procédure permettant de déterminer si une personne ou une chose est effectivement la personne ou la chose qu'elle est censée être.
Droits à privilège / Droit administrateur	Ensemble de droits permettant de réaliser des actions (notamment d'administration) bloquées pour un utilisateur du SI (e.g. : installer un logiciel sur son poste de travail est une action d'administration nécessitant des droits à privilège)
Traçabilité	Procédure visant à tracer l'exécution d'un processus.
Habilitation	Ensemble des droits d'accès d'un utilisateur, relatifs à des données ou à des programmes spécifiques.
Utilisateur	Toute personne ayant accès, dans le cadre de l'exercice de son activité professionnelle, aux moyens informatiques et de communications du groupe, quel que soit son statut.
Partenaire externe au SI	Toute personne physique ou organisme étranger à l'entreprise offrant des services/prestations et ayant un accès au système d'information
Droit d'en connaître	Droit d'une personne à accéder à une information elle a un réel besoin professionnel.

La Charte a été validée en séance Comex le 2 novembre 2021 et insérée dans le Code de Conduite du groupe Sodiaal.