ADMINISTRATION CHARTER

V 0.9.3

SODIAAL

Coopérative Laitière Française

2021

I. Introduction

1. Preamble

This charter supplements the User Charter and applies to all users of the group and more specifically to those with administrator status.

An administrator is a person, **whether or not employed by Sodiaal**, in charge of the proper functioning of the IS. He or she is responsible for his or her area of activity where he or she will carry out various actions made possible by specific rights known as "privileges".

The various administrators are:

- System administrator
- Network administrator
- Database administrator
- Application administrator (Cloud, On Premise)
- Infrastructure Element Administrator
- Administrator of collaborative tools (Teams, Intranet, etc.)

In addition, every user with **privilege/administrator rights on their workstation** is an administrator and must apply this policy.

The objectives of this charter are to:

- Specify **the rights and duties of the Administrator** in the exercise of his or her function or professional activity.
- **Avoid any form of abuse of the use of IT tools** and constitutes **a binding reference** document within Sodiaal.

This charter is composed of a set of information on **(I)**, mandatory measures **(O)** and restrictions **(R)** which apply according to the scope of application:

2. Scope of application

This charter is addressed to all administrators on all or part of the Sodiaal IS, whether they are:

- Internal or external: Employee, Trainee, Temporary worker, Service provider, Work placement
- Temporary or permanent: Fixed-term contract, Permanent contract, Service contract

This charter is addressed not only to the administrators, but also to any line manager and/or operational manager who has the duty to make the charter known and respected by his or her teams in the execution of the administration tasks entrusted to them.

II. Administrators' rights

1. Users with extended rights

O1	In order to carry out the actions in his or her scope, the administrator has an account with privileged rights. This account has the following features: • Identification of the account as privileged (registered account) • Traceability of actions carried out. As such, this account may require stronger authentication measures than standard user accounts.
R1	Administrator rights cannot be set on generic or shared accounts.
I1	In particular, the IS administrator can perform the following tasks: • Isolate, shut down or reconfigure user accounts, equipment or IT applications that could compromise the security of the entire Sodiaal IS; • Carry out technical checks on database, logging or configuration files, in order to detect any anomaly or security incident that could affect the proper functioning of Sodiaal's IS; • Process (detection, analysis, eradication, filtering, etc.) any computer flow presenting potential security risks (virus, intrusion, use of prohibited software, etc.).
I2	In the event of identified abnormal behaviour or suspicions about the legitimacy of actions in relation to the activity of Sodiaal users, the administrators may be required to carry out the following actions after informing the management and/or users, in accordance with the organisation in place: • Prolonged interruption in service: • Interruption of any user task in the event that excessive use of resources impairs the proper functioning of the system (with or without notice, depending on the urgency of the problem); • External storage or compression of excessively large files or files not directly related to the business (with or without prior notice) in the case of deterioration in service; • Interrupting work sessions that are inactive for too long. • Temporary blocking of an account and temporary revocation of access
R2	The use of the administrator account to carry out daily actions on the IS (e-mail consultation, Internet browsing, office automation, etc.) is prohibited. For these actions the administrator has a standard account. In addition to this, he or she has his or her own administrator account dedicated to administration actions.

2. Use of specific software and hardware

I3	The IS administrators identified by Sodiaal may be required to use specific software that is not authorised to users of Sodiaal's IS, in particular software enabling scans to be made on the network or on a group workstation.
O2	The use of remote maintenance software to take remote control of a user's workstation requires the systematic agreement of the user.
O3	The installation or updating of components on the IS must follow the following requirements: • Only from the official sources of the software publisher; • After checking the integrity of the installed binaries using cryptography (digital signature of the files based on a hash: SHA2, SHA256, SHA1, etc.).

III. The duties of directors

1. General information

O4	The administrator must comply with the following: • User charter • IS Charter (especially in case of installation of tools on the workstation) • Existing policies/procedures • Applicable laws/regulations • Confidentiality/non-disclosure agreements
O5	All administrators must keep the authentication of their personal accounts, as well as the technical accounts of which they have knowledge in carrying out their task, strictly confidential.
O6	Administrators must ensure that they have the prior approval of the owner of an application or information before granting access rights to a user.
O7	Administration sessions and tools should be closed when administration actions are performed.
O8	The administrator is responsible for the implementation of the authorisations giving access to confidential data. These authorisations should be in line with the right-to-know principle.

R3	The administrator should not take instructions from an unauthorised person. They must inform their line manager of any non-legitimate request. His or her line management may authorise him or her to perform this handling. The administrator must not implement requests that appear to him to be contrary to this charter, to good practice in terms of health and IT security, or to the laws in force, but must refer to his hierarchy and to the person responsible for the security of Sodiaal's IS.
R4	The administrator must not circumvent established security procedures, and in particular must not: • Disable authentication and traceability mechanisms on his or her own initiative • Undermine the integrity of log files.
R5	Administrators must not abuse their privileges and must limit their actions to the computer resources for which they are responsible, in accordance with the purpose of their mission. In particular, the administrator must not: • Use assets in a misleading way, for personal use • Grant additional rights to the IS.
O9	The administrator must respect his or her commitments of discretion - confidentiality. As such, he or she must not use information that he or she may come into contact with in the course of his or her duties outside the group.

2. Incident management

O10	In the event that an incident occurs, the administrator shall informs his or her line manager and follow the established incident management process.
O11	In the event that the incident calls into question the security of the group in one way or another, the administrator will ensure that all the "history" necessary for the resolution of the incident and any subsequent investigation are kept and will inform the Sodiaal ISSM.
O12	The administrator is subject to a duty to warn. In the event that an administrator detects an event, action or behaviour that is contrary to the user charter, this charter or good practice in terms of computer hygiene and security, he or she is obliged to alert his or her superiors and the ISSM.
R6	The administrator is subject to a duty of confidentiality and may not communicate internally or externally about an incident of which he or she is aware, apart from exchanges with the persons affected. Resolution teams and notified persons are considered impacted.

O13	The administrator's duty of confidentiality must be included in his or her employment or service contract.
I4	Copies made in the context of legal proceedings must comply with the applicable legal framework: copies with evidential value, conservation according to the necessary periods.

3. Data manipulation

O14	If an administrator becomes aware of the password associated with a user ID (e.g. as part of a reset), the administrator should remind the user of their duty to change the password.
R7	The administrator should only be aware of information for which he or she has a need to know, or with a formal waiver from his or her line manager in compliance with rule O6.
R8	The administrator is not authorised to take cognisance of users' personal data (including login and password), except in special cases provided for by law (e.g. letters rogatory, judicial investigations).
R9	The administrator is not authorised to extract or copy any data from the information system outside the strict exercise of his or her task. Any extraction or copy that is necessary to assist in the diagnosis of an incident must be deleted under the responsibility of the administrator and within the maximum timeframe of the resolution of the incident.
R10	Copying Sodiaal data onto equipment belonging to a third party is prohibited.
O15	Before transferring data outside the group, the administrator should check that the recipients, tools and procedures used are appropriate for the supposed confidentiality of the data.

IV. Check

O16	Any operation impacting the security perimeter (IS, application, infrastructure, etc.) must be recorded (follow-up, history). The administrator is therefore responsible for the traceability of his or her actions, in particular the opening, monitoring and documentation of tickets, production releases and any changes in his or her area of activity.
O17	It is the responsibility of the administrators to draw up and transmit incident reports, indicating any event that calls into question the quality and security of Sodiaal's IT resources. He or she is also responsible for reporting any breach of this charter and the charter for the use of computer resources.
I5	Sodiaal reserves the right to check, automatically or by manual checks, the conformity of the authorisations in place and the accesses made. These checks may also target the strength of the passwords used.

V. Applicable sanctions

R11	Failure to comply with or violation of the rules and obligations of this charter shall engage the responsibility of the administrator and shall constitute a fault liable to disciplinary sanctions, as described by the process defined in the internal regulations and in the charter for the use of IT resources.
R12	Furthermore, Sodiaal may be required to inform the competent authorities of any criminal acts committed by the directors (e.g.illicit activity on the Internet). Similarly, in the context of legal proceedings, the competent authorities may be required to take cognisance of the log files. In addition, the personal liability of the director may be sought in the case of: • Damage caused to a third party or to Sodiaal; • Criminal offences committed within the group or using the resources made available to him or her.
R13	Where the administrator in question is an external party or any user of a service provider or subcontractor, the administrator's failure to comply with the charter may result in the latter's expulsion from the premises and the immediate withdrawal of his or her access rights.

VI. Glossary

Words	Definitions
IS	Information System:
ISSM	Information Systems Security Manager
Security incidents	A security incident is an unplanned event that affects the integrity or confidentiality of IS data or damages Sodiaal's image
Administrator	The administrator is a person responsible for the proper functioning of the IS. He or she is responsible for his or her area of activity where he or she will carry out various actions made possible by specific rights known as "privileges" or administrator rights.
Authentication	A procedure for determining whether a person or thing is in fact the person or thing it purports to be.
Privilege rights/ Administrator rights	Set of rights making it possible to carry out actions (notably administration) blocked for a user of the IS (e.g. installing software on a workstation is an administrative action requiring privileged rights)
Traceability	A procedure for tracking the execution of a process.
Permissions	A set of user access rights to specific data or programs.
User	Any person who has access to the group's IT and communications resources in the course of his or her professional activity, regardless of status.
External partner to the IS	Any natural person or organisation outside the company offering services and having access to the information system
Right to know	A person's right to access information for which they have a genuine business need.

The Charter was validated at the Comex meeting on 2 November 2021 and included in the Sodiaal Group Code of Conduct.