

Mission Sécurité des Systèmes et d'Information



POUVOIR ADJUDICATEUR

FranceAgriMer

Adresse du siège : 12 rue Henri Rol-Tanguy - Montreuil sous Bois (93)

Adresse postale : FranceAgriMer -TSA 20002 -93555 Montreuil sous Bois cedex

ANNEXE 5 – CHARTE DE SECURITE DES ADMINISTRATEURS DES SYSTEMES D'INFORMATION

FOURNITURE DE SERVICES D'ASSISTANCE
INFORMATIQUE

REFERENCE INTERNE DU MARCHE : SI-U_PROD2026-CDS

CHARTRE DE SECURITE DES ADMINISTRATEURS DES SYSTEMES D'INFORMATION

Les systèmes d'Information (SI) de FranceAgriMer sont placés sous la responsabilité opérationnelle des « administrateurs ».

Le terme « Administrateur » désigne toute personne (agent de FranceAgriMer ou prestataire) chargée de l'administration ou de l'exploitation des ressources des SI de FranceAgriMer.

Pour FranceAgriMer, on distingue cinq profils d'administrateurs :

- les administrateurs « systèmes », responsables de l'exploitation des systèmes informatiques (Serveurs, systèmes de stockage, référentiels, moyens de messagerie, moyens de sauvegarde etc.) ;
- les administrateurs « réseau et télécommunications », responsables de l'exploitation des moyens de communication et des infrastructures de transport de l'information (câblage, réseau locaux, télécommunications informatiques, internet, téléphonie etc.) ;
- les administrateurs « sécurité », responsables de l'exploitation des moyens de protection du système d'informations et des infrastructures de sécurité ;
- les administrateurs de ressources utilisateurs, responsables de l'exploitation des moyens mis à disposition des utilisateurs (station de travail, ressources bureautiques, support et assistance, inventaire etc.) ;
- les administrateurs d'applications, responsables de l'exploitation et de la maintenance des applications et des bases de données ;

Les administrateurs disposent de « privilèges » qui leur sont accordés pour accomplir leur mission et d'habilitations spécifiques les distinguant de la communauté des utilisateurs conventionnels.

C'est pourquoi, il convient de préciser les règles à suivre en la matière.

La « Charte de sécurité des administrateurs des systèmes d'information » définit les droits et les devoirs applicables spécifiquement à l'ensemble des personnes chargées des tâches d'administration ou d'exploitation des ressources des SI de FranceAgriMer.

Ce dispositif vient compléter la « Charte d'utilisation des ressources informatiques et des moyens de télécommunication » existante qui s'applique à l'ensemble du personnel.

1 Les droits de l'administrateur

Les droits de l'administrateur découlent des missions qui lui sont dévolues.

Les missions de l'administrateur sont définies dans la fiche de poste, s'il est un agent de FranceAgriMer. Elles sont également précisées dans les contrats souscrits par l'établissement, si l'administrateur est un intervenant prestataire.

Il s'agit principalement **d'assurer le bon fonctionnement du SI de l'établissement et de veiller à la sécurité des ressources techniques placées sous sa responsabilité d'exploitation** (composants système, composants de réseau et de télécommunication, composants de sécurité, applications informatiques, bases de données, postes de travail utilisateurs et téléphonie).

Afin de conduire les actions quotidiennes relevant de son activité de gestion (configuration, supervision, maintenance, évolution, support, etc.), **l'administrateur dispose de « privilèges » et de droits d'accès spéciaux sur les ressources** du domaine d'intervention qui est le sien.

Les risques associés aux privilèges qui leur sont accordés sont principalement :

- l'accès à des informations dont il n'est pas le destinataire, certaines étant confidentielles (bases de données, documents sur les postes de travail utilisateurs, etc.), ou à caractère personnel (courriels, fichiers personnels des utilisateurs, etc.) ou encore relatives aux activités des utilisateurs (caractéristique d'utilisation de la messagerie et de l'Internet, données de connexion aux ressources du système d'information, etc.) ;
- la réalisation d'actions potentiellement dangereuses pour la sécurité des Systèmes d'Information : modification ou contournement de mécanismes de protection, création ou modification de comptes utilisateurs, destruction ou modification de fichiers.

L'administrateur agit sous l'autorité de son responsable hiérarchique. Il applique les consignes formelles qui lui ont été transmises et intervient dans le cadre strict de procédures préalablement définies par l'établissement. Il est toutefois responsable des interventions qu'il réalise sur l'environnement technique qu'il exploite.

Dans le cadre des missions qui lui sont confiées, il est amené à :

- contrôler la bonne utilisation des ressources et intervenir sur les environnements techniques où résident les processus de travail des utilisateurs ;
- examiner des données dans le cadre de la surveillance de la bonne marche du système qu'il a en charge ;
- isoler, arrêter, reconfigurer des équipements ou des applications informatiques s'il y détecte une compromission ou un risque ;
- traiter tout processus informatique présentant des risques de sécurité et notamment en matière de virus, d'intrusion ou d'utilisation frauduleuse de ressources informatiques ;
- utiliser des fichiers journaux et accéder aux informations privées uniquement à des fins de diagnostic et d'administration du système ;
- procéder à des opérations de capture et d'injection de données sur les supports de transmission de la responsabilité de FranceAgriMer, en vue de réaliser un diagnostic, la correction d'un problème et /ou de s'assurer du bon fonctionnement (point spécifique pour l'administrateur de ressources de réseau et de télécommunication) ;
- procéder à des vérifications techniques et des audits sur les ressources, afin de déceler toute anomalie ou incident de sécurité qui pourrait porter atteinte au bon fonctionnement et à la sécurité des SI de l'établissement, conformément aux dispositions de la Charte d'utilisation des ressources informatiques et des moyens de télécommunication de FranceAgriMer.

2 Les devoirs de l'administrateur

Les ressources informatiques et les réseaux de communication font partie intégrante du patrimoine de FranceAgriMer. A ce titre, toutes les informations situées sur les systèmes ou véhiculées sur les supports de transmission doivent rester intègres et disponibles, tout en bénéficiant d'un niveau de confidentialité adapté à leur sensibilité.

Les devoirs de l'administrateur découlent des responsabilités qui lui sont confiées.

⇒ L'administrateur est responsable des interventions qu'il réalise.

Il doit :

- respecter les règles de déontologie liées à sa fonction et les dispositions légales et réglementaires qui lui sont applicables ;
- protéger les informations accessibles depuis son environnement en respectant les dispositifs, les règles de sécurité et les procédures de FranceAgriMer, sans chercher à les modifier ou à les contourner explicitement ou implicitement ;
- contribuer à l'amélioration du fonctionnement et de la sécurité des outils qu'il administre ;
- respecter les règles de séparation des fonctions et des responsabilités définies au sein de sa structure ;
- s'assurer de la disponibilité des licences et obtenir l'autorisation de sa hiérarchie avant de procéder à des installations de logiciels.

⇒ L'administrateur est soumis au secret professionnel et aux règles de la confidentialité.

Il ne doit pas :

- prendre connaissance des données personnelles des utilisateurs, sauf en cas d'application des dispositions exceptionnelles prévues par la Charte d'utilisation des ressources informatiques et des moyens de télécommunication de FranceAgriMer ;
- faire état et utiliser à des fins personnelles, les informations qu'il peut être amené à connaître dans le cadre de ses activités ;
- autoriser l'accès aux informations personnelles à des tiers sauf sur demande explicite du (ou des) propriétaire(s) d'informations, dans le cadre de procédures formalisées ou dans les cas particuliers prévus par la loi ;
- se connecter à une ressource en dehors du cadre prévu par ses missions.

⇒ L'administrateur observe strictement les règles de sécurité et les limites fixées à ses interventions.

A ce titre, il prend ses consignes auprès de son responsable hiérarchique, écarte toute requête hors du cadre hiérarchique lui paraissant inappropriée, et en informe sa hiérarchie.

Il ne doit pas :

- abuser de ses privilèges, et ses actions se limitent 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 ;
- contourner les procédures de sécurité établies, et en particulier désactiver de sa propre initiative les mécanismes de traçabilité, et porter atteinte à l'intégrité des fichiers de journalisation ;
- utiliser des logiciels ne faisant pas partie des standards approuvés par l'établissement, sauf en cas d'autorisation préalable et explicite du responsable hiérarchique.

⇒ L'administrateur contribue aux actions de sécurité mises en place dans l'établissement.

Il doit :

- signaler toute anomalie constatée et a fortiori tout incident de sécurité selon la procédure en vigueur ;
- informer directement le Responsable Sécurité des Systèmes d'Information de FranceAgriMer, s'il s'agit d'un cas grave de non respect de la Charte d'utilisation des ressources informatiques et des moyens de télécommunication de la part d'un utilisateur.

⇒ L'administrateur veille au respect de la présente charte au niveau de son équipe et des tiers intervenant sous son autorité.

Il doit :

- diffuser la présente charte à tous les acteurs de l'exploitation qu'il encadre (internes et prestataires) et aux intervenants de projets, de la maintenance et en règle générale pour toutes interventions d'assistance à l'administration et veiller au respect des règles énoncées ;
- tenir informé ses adjoints et les opérateurs d'exploitation des problèmes dont il a connaissance ;
- signaler toute attitude inappropriée à sa hiérarchie.

⇒ L'administrateur participe activement à la gestion des incidents.

En cas d'incident d'exploitation, il doit :

- appliquer la procédure de signalement de l'incident et de remontée de l'information vers sa hiérarchie et vers la mission SSI ;
- qualifier les causes et les conséquences de l'incident ;
- participer à la résolution de l'incident et constituer le dossier technique de l'incident.

⇒ L'administrateur s'assure de la protection des éléments de privilèges qui lui sont accordés.

Il doit :

- observer les règles de sécurité en vigueur visant à protéger l'utilisation des comptes et des privilèges qui lui ont été attribués (les droits confiés à un administrateur sont strictement personnels et inaccessibles) ;
- respecter les procédures de mise en œuvre des comptes de service et limiter leur utilisation aux activités directement liées aux tâches d'administration ou d'exploitation dont il a la charge ;
- s'assurer régulièrement de la protection des postes de travail à partir desquels il exerce ses activités ;
- limiter l'usage d'Internet via un compte à privilèges aux seuls accès nécessaires à la réalisation des missions.

3 La revue de l'activité

L'activité des administrateurs peut faire l'objet de revue dans le cadre des dispositions de contrôle interne pour s'assurer du respect des règles et des procédures d'exploitation définies au sein de son service.

A ce titre, l'administrateur s'engage à se rendre disponible pour ces vérifications et ne pas entraver ces contrôles. Il devra faciliter l'accès aux moyens de traces des systèmes et équipements qu'il administre et fournir en toute transparence toutes les informations utiles à ces missions de vérification.

Tout évènement permettant de relever une activité inappropriée, la dissimulation de trace ou de preuve d'activité expose l'administrateur aux sanctions prévues et détaillées au chapitre 4 de la présente charte.

4 Le respect de la législation et de la présente charte et les sanctions

Les limites de l'intervention de l'administrateur sont fixées de manière générale par la législation en vigueur et par la présente Charte.

Le fait d'enfreindre ou de négliger l'application des règles mentionnées dans la présente charte fait encourir des risques à l'établissement.

Tout administrateur des ressources de l'établissement s'engage formellement à respecter en toutes circonstances la législation en vigueur et les règles de la présente charte (cf. formulaire - annexe).

L'administrateur est informé qu'un usage inapproprié des ressources est susceptible d'engager sa propre responsabilité.

En cas de non respect de la législation en vigueur et des dispositions de la présente charte, l'administrateur sera tenu pour responsable de ses actes et pourra encourir les sanctions disciplinaires prévues au niveau de l'établissement ainsi que toute autre sanction découlant d'une action judiciaire civile ***ou pénale*** prévue par la loi.

En aucun cas, l'administrateur ne peut être contraint par sa hiérarchie à enfreindre la loi.

L'administrateur est vivement invité à prendre connaissance des principales dispositions légales en vigueur, rappelées ci-dessous :

- la loi n° 7817 du 06/01/1978, modifiée, relative à l'informatique, aux fichiers et aux libertés,
- la loi n° 8819 du 05/01/1988, modifiée, (loi « Godfrain »), sur la fraude informatique,
- la loi n° 92597 du 01/07/1992, modifiée, (« code de la propriété intellectuelle »),
- la loi n° 2004575 du 21/07/2004, modifiée, (loi « LCEN »), pour la confiance dans l'économie numérique.
- Le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

Et à titre d'information :

- la loi n° 92685, du 22/07/1992, portant réforme des dispositions du code pénal relatives à la répression des crimes et délits contre les personnes,
- la loi «relative aux infractions aux règles de cryptologie» du 29/12/1990 modifiée le 26/7/1996,
- la loi n° 94548 du 1er juillet 1994 (Journal officiel du 2 juillet 1994), relative au traitement de données nominatives ayant pour fin la recherche dans le domaine de la santé et modifiant la loi no 7817 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés,
- la loi n°2006-64 du 23 janvier 2006, relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers,
- l'article 22615 du code pénal sur l'atteinte au secret des correspondances.