REGLEMENT INTERIEUR DE L'URSSAF ILE DE FRANCE

SOMMAIRE

Page 1 : INTRODUCTION

Page 2 : REGLEMENT INTERIEUR

Page 20 : ANNEXE 1 CHARTE INFORMATIQUE

INTRODUCTION

Ce document constitue le règlement intérieur de l'Urssaf Ile de France dont les dispositions s'imposent à l'ensemble du personnel.

Il comporte une annexe, dotée de la même force juridique et faisant partie d'un ensemble indivisible.

Urssaf
Île-de-France

SOMMAIRE

I – PREAMBULE

ARTICLE 1 : OBJET ET CHAMP D'APPLICATION**II –**

REGLES RELATIVES A LA DISCIPLINE ARTICLE 2 :

DISCIPLINE GENERALE

ARTICLE 3 : PREVENTION DES CONFLITS D'INTERET

ARTICLE 4 : CIRCULATION DANS L'ORGANISME

ARTICLE 5 : UTILISATION DU MATERIEL DE L'ORGANISME

ARTICLE 6 : UTILISATION DE LA MESSAGERIE ELECTRONIQUE ET DES OUTILS INFORMATIQUES – ACCES A INTERNET

ARTICLE 7 : HORAIRES DE TRAVAIL

ARTICLE 8 : ABSENCES

ARTICLE 9 : INTERDICTION ET SANCTION DU HARCELEMNT MORAL ET SEXUEL

ARTICLE 10 : INTERDICTION DE TOUTE PRATIQUE DISCRIMINATOIRE AINSI QUE DE TOUT AGISSEMENT SEXISTE

ARTICLE 11 : PROCEDURE DE PREVENTION CONTRE LE HARCELEMENT MORAL OUSEXUEL, LES DISCRIMINATIONS ET LES COMPORTEMENTS SEXISTES

ARTICLE 12 : RESPECT DE LA NEUTRALITE ET DE LA LAICITE DU SERVICE PUBLIC

III – SANCTIONS ET GARANTIES DE PROCEDURE

ARTICLE 13 : SANCTIONS DISCIPLINAIRES ARTICLE 14

: PROCEDURE DISCIPLINAIRE

ARTICLE 15 : GARANTIE DES DROITS DES SALARIES

IV – SANTE, HYGIENE ET SECURITE

ARTICLE 16 : SANTE ARTICLE

17 : HYGIENE ARTICLE 18 :

SECURITE

ARTICLE 19 : MODALITES D'EXERCICE DU DROIT D'ALERTE ET DE RETRAITARTICLE 20 :

CONDUITE DES VEHICULES

V – ENTREE EN VIGUEUR ET MODIFICATIONS DU REGLEMENT

ARTICLE 21 : DATE D'ENTREE EN VIGUEUR

I – PREAMBULE

ARTICLE 1 : OBJET ET CHAMP D'APPLICATION

Le présent règlement a pour objet, conformément aux dispositions des articles L 1321-1 et suivants du code du travail, de :

- Préciser l'application à l'entreprise de la règlementation en matière de santé et de sécurité, notamment les instructions prévues à l'article L. 4122-1,
- Déterminer les règles générales et permanentes relatives à la discipline,
- Rappeler les garanties accordées aux salariés en matière de sanctions disciplinaires,
- Rappeler les dispositions relatives à l'interdiction du harcèlement sexuel et de toute pratique de harcèlement moral.

Il s'applique :
- à tous les salariés de l'Urssaf Ile de France en quelque endroit où ils se trouvent (bureaux, cafétérias, parkings, etc.),
- pour les mesures relatives à la santé et à la sécurité, aux salariés temporaires, aux salariés des entreprises extérieures et aux stagiaires présents dans l'entreprise et, plus généralement, à toute personne présente dans les locaux de l'Urssaf Ile de France àquelque titre que ce soit,
- aux représentants du personnel, dans les respect des conditions et modalités fixés par la législation pour l'exercice de leurs mandats.

Les notes de service portant prescriptions générales et permanentes dans les matières relevant du domaine du règlement intérieur sont considérées comme des adjonctions à ce règlement et soumises au même régime juridique.

Le présent règlement ne remet pas en cause le règlement intérieur type, ce dernier étant un texte conventionnel complétant la convention collective, ainsi que le prévoit son article 62.

Ce document est communiqué à chaque nouveau salarié, lors de son embauche, pour qu'il en prenne connaissance.

II – REGLES RELATIVES A LA DISCIPLINE

ARTICLE 2 : DISCIPLINE GENERALE

2-1 Exécution des activités professionnelles

Dans l'exécution des tâches qui lui sont confiées, chaque salarié est tenu de respecter les instructions qui lui sont données par ses supérieurs hiérarchiques, notamment dans les conditions et délais prescrits, l'employeur mettant à sa disposition les moyens nécessaires à la mise en œuvre de ces instructions.

2-2 Secret professionnel et confidentialité

Chaque salarié de l'Urssaf Ile de France est tenu au secret professionnel et à une obligation de confidentialité vis-à-vis des tiers.

ARTICLE 3 : PREVENTION DES CONFLITS D'INTERET

La nature des activités exercées au sein de l'Urssaf peut créer pour les collaborateurs des situations présentant un risque de conflit d'intérêt. Un conflit d'intérêt désigne toute situation avérée ou apparente dans laquelle un salarié possède un intérêt direct ou indirect pouvant influer sur la manière dont il s'acquitte de ses fonctions dans l'entreprise. Concrètement, il s'agit de situation d'interférence entre notre mission de service public et les intérêts privés que chacun peut avoir.

Afin de protéger les salariés et l'organisme contre tout risque de prise illégale d'intérêt, chaque salarié effectue une déclaration précisant la liste des comptes dont il est titulaire ou de ceux avec lesquels il pourrait être en relation, pouvant générer pour lui une situation de conflit d'intérêt et dont il ne souhaite pas assurer la gestion. Cette déclaration est actualisée suite à tout changement affectant les listes de comptes évoquées ci-dessus. L'employeur peut s'assurer à tout moment que les interventions des salariés sur les comptes identifiés ne dérogent pas aux règles de la branche en matière de gestion des comptes cotisants.

Par ailleurs chaque salarié de l'Urssaf Ile de France, à quelque niveau que ce soit, en présence d'un conflit d'intérêt sur un dossier ou une situation qu'il a à traiter, doit le signaler immédiatement à son supérieur hiérarchique, ceci à des fins de protection du salarié lui- même et de l'action de l'Urssaf. Ce signalement doit être réalisé sur chaque conflit d'intérêt avant tout traitement. Il n'est pas nécessaire de détailler l'origine du conflit d'intérêt qui peut relever de la sphère privée. Le signalement peut être effectué oralement dans un premier temps, en cas d'hésitation de la part du salarié confronté à une situation particulière. Ce premier échange oral lui permettra notamment de bien préciser avec son supérieur hiérarchique ce qui relève réellement d'un conflit d'intérêt.

Pour prévenir l'apparition de tout risque de conflit d'intérêt, et garantir la sécurité, la confidentialité et l'intégrité des données des cotisants comme des salariés, les collaborateurs limitent l'accès aux informations situées sur les applications et référentiels à la seule finalité de leur mission professionnelle. La consultation de leurs propres données est proscrite.

En cas de situation avérée de conflits d'intérêts, ce signalement doit être formalisé et signalé au supérieur hiérarchique par écrit. Cet écrit est conservé par le salarié et son supérieur hiérarchique. En cas d'absence du supérieur hiérarchique direct, le signalement est fait au n+2. A réception du signalement du conflit d'intérêt, le supérieur hiérarchique réattribue le dossier à un autre salarié, non exposé à un conflit d'intérêt. La décision de gestion ainsi que l'identité du salarié auquel le dossier est réattribué sont formalisées et transmis à la direction maîtrise des risques à des fins de centralisation et de suivi général.

Tout salarié qui se soustrait à ce devoir d'alerte et effectue des interventions sur un compte pour lequel son objectivité peut être mise en cause s'expose à l'une des sanctions prévues par le présent règlement.

ARTICLE 4 : CIRCULATION DANS L'ORGANISME

4-1 Salariés de l'organisme

Les salariés de l'organisme sont munis d'un badge nominatif portant une photo d'identité qu'ils doivent conserver sur eux en permanence dès lors qu'ils sont dans l'enceinte de l'organisme, quel que soit le site.

Afin de pouvoir identifier rapidement et avec certitude les personnes faisant partie de l'organisme, il peut être demandé aux salariés circulant dans l'organisme de présenter leur badge.

Ces contrôles permettent, dans le cadre de la politique de sécurité de la branche Recouvrement et de sûreté de nos bâtiments, d'identifier rapidement et avec certitude les personnels faisant partie de l'organisme et de leur garantir la sécurisation de l'accès au poste de travail.

4-2 Personnes extérieures

Le personnel n'est pas autorisé à introduire ou à faire introduire, dans l'organisme, des personnes étrangères à celui-ci, sauf autorisation exceptionnelle du responsable du site ou de son représentant.

Sous réserve des dispositions des articles L 2142-10 et L 2325-13 du Code du travail relatives aux droits de la représentation du personnel, l'accès aux locaux de l'organisme et leséjour dans les locaux de toute personne étrangère au service sont soumis à une autorisation préalable ou à une prise de rendez-vous.

Après s'être identifiée par tout moyen représentatif (carte professionnelle, carte d'identité, …), la personne extérieure à l'organisme peut circuler dans les locaux, soit après remise d'un badge de circulation comportant son identité professionnelle (nom, prénom organisme ou entreprise concernée), soit en étant accompagnée par un salarié de l'Urssaf.

La personne extérieure au service s'engage à respecter les prescriptions en matière de sécurité, notamment du système d'information, et de confidentialité des données auxquelles elle pourrait avoir accès au cours de sa mission.

ARTICLE 5 : UTILISATION DU MATERIEL DE L'ORGANISME

5-1 Le personnel n'est pas autorisé à se faire expédier correspondance et colis personnels à l'adresse de l'entreprise (hors livraison de déjeuner à l'entrée des locaux de l'entreprise).

5-2 Chaque salarié est tenu de conserver en bon état, le matériel qui lui est confié (photocopieurs, micros ordinateurs, téléphones fixes et mobiles, outillage, …) en vue de l'exécution de son travail.

De même, il ne doit pas utiliser ledit matériel à d'autres fins sans autorisation.

S'agissant de leur utilisation à des fins privées, si une certaine tolérance est admise, le caractère répétitif d'un tel comportement, son temps ou sa durée, malgré un rappel de la part de l'employeur, pourraient légitimer une sanction, dans la mesure où l'organisme est en droit

d'attendre d'un salarié qu'il exécute son contrat de travail dans le respect d'une obligation générale de loyauté.

5-3 Les communications téléphoniques ou l'usage d'internet à des fins personnelles ne sont tolérés qu'à la condition qu'une telle utilisation demeure raisonnable, qu'elle ne soit pas préjudiciable à l'employeur et qu'elle soit limitée aux nécessités de la vie personnelle et familiale.

5-4 Toute dégradation volontaire du mobilier et du matériel appartenant à l'organisme sera passible de sanctions disciplinaires.

5-5 Il est interdit d'emporter des objets appartenant à l'organisme sauf autorisation.

5-6 En cas de nécessité, notamment en cas de disparitions renouvelées et rapprochées d'objets et de matériel appartenant à l'entreprise, il pourra être procédé de manière non systématique et ponctuellement à des fouilles du contenu des vestiaires ainsi que des effets et objets personnels du salarié, dans des conditions qui préservent la dignité et l'intimité de la personne.
Le salarié sera averti du droit de s'opposer à un tel contrôle. Il est en droit d'exiger la présence d'un témoin salarié ou d'un représentant du personnel lors de cette vérification. En cas de refus de l'intéressé, la direction devra faire appel à un officier de police judiciaire.

5-7 Il est interdit de lacérer ou détruire les affiches ou notes de service régulièrement apposées sur les panneaux muraux appropriés ainsi que de procéder à un affichage en dehors des panneaux réservés.

5-8 Lors de son départ de l'organisme, le salarié restitue le matériel mis à sa disposition - tels que ordinateur ou téléphone portable, token notamment.

ARTICLE 6 : UTILISATION DE LA MESSAGERIE ELECTRONIQUE ET DES OUTILS INFORMATIQUES - ACCES A INTERNET

Chaque salarié de l'organisme est tenu de respecter les dispositions de la charte informatique annexée au présent règlement.

ARTICLE 7 : HORAIRES DE TRAVAIL

7-1 Dispositions générales

Les salariés sont tenus de respecter les dispositions en matière d'aménagement du temps de travail et d'horaires variables qui leur sont applicables.

Le dispositif d'horaires variables doit être mis en œuvre de façon à garantir le bon fonctionnement des services et la mission de service public de l'organisme.

Tout salarié qui le souhaite peut solliciter le bénéfice d'une formule de temps choisi.

Cette demande est examinée par le responsable hiérarchique.

Dès lors qu'un salarié a badgé, il est en situation de travail effectif et doit se rendre aussitôt à son poste de travail. A ce titre, conformément à l'article L 3121-1 du Code du travail, « *la durée du travail effectif est le temps pendant lequel le salarié est à la disposition de l'employeur et se conforme à ses directives sans pouvoir vaquer librement à des occupationspersonnelles* » (repas, activités extra-professionnelles, etc.).

7-2 Dispositions particulières (DSI, téléopérateurs)

Au sein de la Direction des Systèmes d'Information : Les opérateurs de l'atelier éditique travaillent en deux équipes, soit de 6h42 à 14h30 et de 13h30 à 21h18.

La plate-forme téléphonique située à Montreuil est ouverte entre 9h00 et 17 h00.

Les téléopérateurs dont le contrat de travail prévoit une durée hebdomadaire de travail de 30h00 travaillent en deux équipes, soit :
- 09 h - 16 h
- 10 h - 17 h

Ils disposent d'une heure pour déjeuner entre 11h45 et 12h45 ou entre 13h00 et 14h00 selon leur horaire de travail.

Une pause de 10 minutes rémunérées leur est accordée après deux heures de travail en continu. Cette pause ne peut être accolée avec l'heure de repas.

Ces dispositions ne sont pas applicables aux téléopérateurs de l'ex-Urssaf de Seine-et- Marne ainsi qu'aux téléopérateurs recrutés après le 1er novembre 2014 dont le contrat de travail prévoit qu'ils effectuent 1607 heures annuelles de travail dont les horaires de travail sont organisés selon un dispositif d'horaires variables.

7-3 Respect des horaires

Tout salarié, qu'il travaille en heures fixes ou en horaires variables, doit respecter les horaires qui lui sont propres. Tout non respect est passible d'une sanction disciplinaire.

Le respect des règles suivantes est impératif :

- Le badge attribué à chaque salarié est strictement nominatif et ne doit par conséquent en aucun cas être utilisé par une autre personne.

- Chaque salarié est tenu, lorsqu'il pénètre ou sort d'un site de l'organisme, de badger ou de débadger. Sauf situation particulière, chaque salarié doit effectuer dans le cas général quatre mouvements par jour sur les plages mobiles prévues à cet effet dans le cadre des horaires auxquels il est soumis.

- La pratique du débadgeage / badgeage simultané est strictement interdite. Le rebadgeage de salarié doit réellement correspondre à une situation où celui-ci est présent sur son poste de travail et en situation de travail effectif.

- Afin de préserver la santé des salariés et de respecter les durées maximales de travail prévues par le Code du travail, le temps de travail effectif ne peut excéder 10 heures au cours d'une même journée. De même, la durée moyenne hebdomadaire du travail effectif

sur une période de 12 semaines consécutives est limitée à 44 heures. Au cours d'une même semaine, la durée hebdomadaire du travail ne peut excéder 48 heures. Le respect de ces seuils est impératif, les salariés n'étant en aucun cas autorisés à les dépasser.

L'oubli d'enregistrement est toléré à titre exceptionnel. Il doit être signalé dans les meilleurs délais par le salarié concerné selon les modalités prévues dans l'outil de suivi des horaires ou, à défaut, par message Lotus à la personne de sa Direction habilitée à la mise à jour des horaires variables et adressé en copie à son responsable hiérarchique.

Les demandes d'absences sur plage fixe doivent faire l'objet d'une demande d'autorisation préalable auprès du responsable hiérarchique du salarié par le biais de l'outil de gestion des absences. Celles-ci doivent revêtir un caractère exceptionnel et avoir une amplitude horaire limitée. Elles ne peuvent concerner que des absences non anticipées (cas d'urgences connues en cours de journée). Ainsi, pour le salarié qui a besoin de s'absenter, l'autorisation d'absence sur plage fixe ne doit pas remplacer la prise d'une demi-journée d'absence imputable sur ses droits (crédit compteur, congé, RTT…).
Des vérifications périodiques sont effectuées par la Direction des ressources humaines, via des requêtes sur les badgeages / débadgeages. Celles-ci seront transmises aux branches et un rappel au règlement intérieur sera effectué par la Direction des ressources humaines, le cas échéant, aux salariés concernés.

7-4 Heures supplémentaires

Les heures supplémentaires sont effectuées conformément aux dispositions légales et conventionnelles applicables.

ARTICLE 8 : ABSENCES

Sous réserve des droits des représentants du personnel, toute absence doit faire l'objet d'une demande d'autorisation préalable.

8-1 Absence pour maladie

Le salarié doit justifier de son absence par l'envoi dans les 48 heures à la Direction des Ressources humaines (le cachet de la Poste faisant foi) d'un arrêt de travail.

Par ailleurs, sauf impossibilité majeure, le salarié doit également prévenir immédiatementson encadrement ou, en cas d'indisponibilité, le secrétariat de son secteur en indiquant la durée prévisible de l'arrêt de travail. Le contact téléphonique direct doit être privilégié avant de recourir à d'autres formes de communication (courriel, SMS).

Enfin, le salarié doit se conformer aux éventuels contrôles médicaux extérieurs effectués à la demande de l'organisme employeur.

8-2 Absence pour un autre motif

Sous réserve des formalités propres à l'exercice du droit syndical ou d'un mandat en tant que membre d'une instance représentative du personnel, tout salarié doit formuler une demande d'absence via l'outil de gestion des absences.

En cas d'absence supérieure à une demi-journée, la demande doit intervenir au plus tard 48 heures avant celle-ci.

Dans l'hypothèse d'une absence imprévue, le salarié doit, le jour même de l'absence,prévenir immédiatement son encadrement ou, en cas d'indisponibilité, le secrétariat de son secteur. Le contact téléphonique direct doit être privilégié avant de recourir à d'autres formes de communication (courriel, SMS).

La régularisation est effectuée dès le retour du salarié.
Cette tolérance pour les absences inopinées présente un caractère strictement exceptionnel. Des absences répétées sans autorisation préalable, après avoir fait l'objet d'un rappel à l'ordre, peuvent donner lieu à l'une des sanctions prévues par le présent règlement.

ARTICLE 9 : INTERDICTION ET SANCTION DU HARCELEMENT MORAL ET SEXUEL

Aucun salarié ne doit subir les ***propos ou comportements répétés*** de harcèlement moral qui ont pour objet ou pour effet une dégradation des conditions de travail susceptible de porter atteinte à ses droits et à sa dignité, d'altérer sa santé physique ou mentale ou de compromettre son avenir professionnel (***Code pénal, art. 222-33-2***).

Aucun salarié ne doit subir des faits :
1° Soit de harcèlement sexuel, constitué par des propos ou comportements à connotation sexuelle répétés qui soit portent atteinte à sa dignité en raison de leur caractère dégradant ou humiliant, soit créent à son encontre une situation intimidante, hostile ou offensante ;
2° Soit assimilés au harcèlement sexuel, consistant en toute forme de pression grave, même non répétée, exercée dans le but réel ou apparent d'obtenir un acte de nature sexuelle, que celui-ci soit recherché au profit de l'auteur des faits ou au profit d'un tiers (Code du travail, art. L 1153-1).
Conformément à l'article L.1153-5 du Code du travail, la direction prendra toutes dispositions nécessaires en vue de prévenir les faits de harcèlement sexuel, d'y mettre un terme et de les sanctionner.

Aucun salarié, aucune personne en formation ou en stage, aucun candidat à un recrutement, à un stage ou à une formation en entreprise, ne peut être sanctionné, licencié ou faire l'objet d'une mesure discriminatoire, directe ou indirecte, notamment en matière de rémunération, formation, reclassement, affectation, qualification, classification, promotion professionnelle, mutation ou renouvellement de contrat, pour avoir subi ou refusé de subir les agissements de harcèlement moral ou sexuel ou pour avoir rapporté de tels faits (Code du travail, art. L 1152-2, L 1153-2, L 1153-3).

Toute disposition ou tout acte contraire est nul de plein droit (Code du travail, art. L 1152-3 et L 1153-4).

Conformément aux articles L 1152-5 et L 1153-6 du Code du travail, est passible d'une sanction disciplinaire tout salarié ayant procédé aux agissements de harcèlement moral ou sexuel.

ARTICLE 10 : INTERDICTION DE TOUTE PRATIQUE OU PROPOS DISCRIMINATOIRE AINSI QUE DE TOUT AGISSEMENT SEXISTE

Conformément à l'article L1132-1 du Code du travail, aucune personne ne peut être écartée d'une procédure de recrutement ou de l'accès à un stage ou à une période de formation en entreprise, aucun salarié ne peut être sanctionné, licencié ou faire l'objet d'une mesure discriminatoire, directe ou indirecte, notamment en matière de rémunération, de mesures d'intéressement, de formation, de reclassement, d'affectation, de qualification, de classification, de promotion professionnelle, de mutation ou de renouvellement de contrat en raison de son origine, de son sexe, de ses mœurs, de son orientation ou identité sexuelle, de son âge, de sa situation de famille ou de sa grossesse, de ses caractéristiques génétiques, de son appartenance ou de sa non-appartenance, vraie ou supposée, à une ethnie ou une nation, de ses opinions politiques, de ses activités syndicales, mutualistes ou associatives, de ses convictions religieuses, de son apparence physique, de son nom de famille ou en raison de son état de santé ou de son handicap.

Des propos de nature discriminatoire exposent ceux qui les tiennent à des sanctions disciplinaires.

Aucun salarié ne peut être sanctionné, licencié ou faire l'objet d'une mesure discriminatoire visée à l'article précédent en raison de l'exercice normal du droit de grève.

Aucun salarié ne peut être sanctionné, licencié ou faire l'objet de mesure discriminatoire pour avoir témoigné des agissements définis aux alinéas précédents ou pour les avoir relatés.

Toute disposition ou tout acte contraire est nul de plein droit.

Conformément à l'article L1142-2-1 du Code du travail, nul ne doit subir d'agissementsexiste, défini comme tout agissement lié au sexe d'une personne, ayant pour objet ou pour effet de porter atteinte à sa dignité ou de créer un environnement intimidant, hostile, dégradant, humiliant ou offensant.

ARTICLE 11 : PROCEDURE DE PREVENTION CONTRE LE HARCELEMENT MORAL OU SEXUEL, LES DISCRIMINATIONS ET LES COMPORTEMENTS SEXISTES.

Tout agent s'estimant harcelé ou faire l'objet d'une discrimination ou d'un comportement sexiste doit le signaler oralement ou par écrit à l'une des personnes de son choix citées ci-dessous :

- sa hiérarchie
- le DRH
- le service de santé au travail
- le service social
- les membres du CHSCT, y compris les membres de droit
- les délégués du personnel.

Le signalement peut également être effectué par un tiers.

Le directeur des ressources humaines qui sera avisé le jour même de ce signalement, recevra alors, dans la semaine, de manière séparée, la victime présumée, puis la ou les personne(s) incriminée(s).

Afin de garantir la confidentialité absolue de cette première phase d'écoute, dénuée de tout formalisme, il ne sera pris aucune note et aucun compte-rendu ne sera rédigé, l'objectif étant

de désamorcer le conflit et de parvenir à une médiation, voire de sceller un accord avec l'assentiment express des personnes en cause, si toutefois il ne s'agit que d'un problème de dialogue, de communication, d'organisation du travail ou de management.

Cependant, en cas d'échec de la médiation, les parties concernées seront avisées qu'une procédure d'enquête va être mise en œuvre.

Cette seconde phase qui permettra de qualifier les faits en droit devra respecter un certain formalisme.

A cette fin, une commission, composée du directeur des ressources humaines ou de son représentant, du médecin du travail et du directeur de branche dans laquelle travaille le plaignant (sous réserve que ce dernier ne soit pas mis en cause par ce dernier), recevra tour à tour les parties préalablement convoquées par écrit, lesquelles pourront se faire assister par une personne de leur choix appartenant à l'entreprise.

Le premier entretien aura lieu avec la victime présumée, les suivants avec la ou les personnes mises en cause.

Les propos tenus seront consignés par écrit.

Par ailleurs, si besoin est, les témoins seront ensuite entendus au cours d'auditions séparées. Après examen des éléments de preuve, trois hypothèses peuvent être envisagées :

- les faits de harcèlement moral ou sexuel ou de discrimination ou de comportement sexiste sont avérés
- les faits de harcèlement moral ou sexuel ou de discrimination ou de comportement sexiste ne sont pas caractérisés et il s'agit plutôt de relations professionnelles difficiles oude stress résultant de difficultés de management ou d'organisation du travail
- on se trouve en présence d'une fausse victime.

A l'issue de cette procédure et selon la situation rencontrée, une action sera engagée, au plus tard dans les six semaines après le signalement.

a) Faits caractérisés de harcèlement moral ou sexuel ou de discrimination ou de comportement sexiste

- mise en place d'une mesure d'accompagnement au profit de la ou des victime(s) du harcèlement moral ou sexuel ou de la discrimination
- mise en œuvre de la procédure au titre de l'article 48 de la Convention CollectiveNationale à l'encontre du ou des coupables en vue d'une sanction disciplinaire
- transmission des informations au procureur de la République avec copie à l'inspecteur du travail. En effet, les faits de harcèlement et de discrimination étant constitutifs d'un délit, le directeur de l'Urssaf Ile de France se rendrait également coupable de délit en cas de non-dénonciation.
- éventuellement, plainte de la victime.

b) Faits non caractérisés de harcèlement moral ou sexuel ou de discrimination ou de comportement sexiste

Selon les cas, il conviendra de mettre en place, en fonction des situations : une action de formation au management, un accompagnement de la personne accusée à tort, une nouvelle organisation de travail ou un changement de lieu de travail.

c) Fausse victime

Toute dénonciation calomnieuse fera l'objet d'une des sanctions prévues par l'article 48 de la Convention Collective Nationale à l'encontre de son auteur.

ARTICLE 12 : RESPECT DE LA NEUTRALITE ET DE LA LAÏCITE DU SERVICE PUBLIC

Sans préjudice des dispositions précitées, les salariés de l'Urssaf Ile de France, organisme privé chargé d'une mission de service public, sont tenus de ne manifester aucun signe contraire au principe de neutralité et de laïcité dans l'exercice de leurs fonctions, en particulier vestimentaires.

Est notamment interdit le port de vêtement ou d'accessoires de manière ostentatoire, positionnant clairement un salarié comme représentant un groupe, une ethnie, une religion, une obédience politique ou religieuse ou quelque croyance que ce soit.

Il est également rappelé que la loi du 11 octobre 2010 interdit le port de tenues destinées à dissimuler le visage dans l'espace public, dont font partie les lieux affectés à un service public.

III – SANCTIONS ET GARANTIES DE PROCEDURE

ARTICLE 13 : SANCTIONS DISCIPLINAIRES

Constitue une sanction toute mesure, autre que les observations verbales, prise par l'employeur à la suite d'un agissement du salarié considéré par lui comme fautif, que cette mesure soit de nature à affecter immédiatement ou non la présence du salarié dans l'organisme, sa carrière ou sa rémunération.

Les sanctions disciplinaires au sens de l'article L1331-1 du Code du travail sont celles énumérées à l'article 48 de la convention collective à l'exclusion de toute amende ou autres sanctions pécuniaires.

- Avertissement,
- Blâme,
- Suspension sans traitement avec maximum de 7 jours ouvrables,
- Rétrogradation,
- Licenciement avec ou sans indemnités

ARTICLE 14 : PROCEDURE DISCIPLINAIRE

Aucune de ces sanctions, antérieure de plus de trois ans à l'engagement des poursuites disciplinaires, ne peut être invoquée à l'appui d'une nouvelle sanction.

a) L'avertissement et le blâme sont prononcés par la Direction sur le rapport écrit, établi par le responsable hiérarchique compétent après un complément d'enquête au cours duquel l'agent en cause est entendu en présence des délégués du personnel. L'agent peut se faire assister par une personne de son choix appartenant au personnel de l'organisme.

La sanction ne peut intervenir moins de deux jours ouvrables ni plus d'un mois après le jour fixé pour l'entretien. Elle doit être motivée et notifiée à l'intéressé.

b) Les trois autres sanctions sont soumises à la procédure suivante, sans préjudice des dispositions spécifiques du code du travail pour ce qui concerne le licenciement :

Lorsque le directeur envisage de prendre l'une de ces trois sanctions, il doit convoquer le salarié en lui indiquant l'objet de la convocation. Au cours de l'entretien, l'agent est entendu en présence des délégués du personnel. Il peut se faire assister par une personne de son choix appartenant au personnel de l'organisme ; l'employeur indique le motif de la sanction envisagée et recueille les explications du salarié.

Il est rappelé que, conformément aux dispositions de l'article 48 de la convention collective :
- le directeur a 5 jours ouvrés maximum à compter du jour de l'entretien pour demander la convocation du conseil de discipline régional.
- le conseil de discipline régional est convoqué par son secrétariat dans un délai de 8 jours suivant la réception de la demande de convocation du directeur et doit se réunir dans les 15 jours suivant la réception de cette demande.
- le conseil de discipline régional ne peut valablement délibérer que si le quorum est atteint dans chaque collège et si la parité est assurée. A défaut, le conseil de discipline régional se réunit à nouveau dans un délai maximum de 8 jours francs et se prononce à la majorité des membres présents.
- les conclusions du conseil de discipline régional sont notifiées par écrit dans les 48 heures au directeur et à l'agent en cause.
- en tout état de cause, la sanction ne peut intervenir avant que le conseil de discipline régional ne se soit prononcé sur la proposition faite par le directeur, le délai total de la procédure ne pouvant excéder un mois à compter de la date de l'entretien.
- le directeur prend sa décision, compte tenu des conclusions du conseil de discipline régional qu'il devra rappeler en tout état de cause dans la notification qui sera faite à l'agent intéressé. La sanction doit être motivée et notifiée à l'intéressé.

En cas de faute professionnelle susceptible d'entraîner le licenciement, le directeur peut prendre une mesure conservatoire de mise à pied à effet immédiat avec traitement pendant un mois au maximum, en attendant que le conseil de discipline régional se soit prononcé, après avoir entendu l'intéressé en présence des délégués du personnel.

Le salarié peut se faire assister par une personne de son choix appartenant au personnel de l'organisme.

En cas de faute grave au sens de la jurisprudence, le directeur peut prendre une mesure conservatoire de mise à pied à effet immédiat et sans traitement, en attendant que le conseil de discipline régional se soit prononcé, après avoir entendu l'intéressé en présence des délégués du personnel. Le salarié peut se faire assister par une personne de son choix appartenant au personnel de l'organisme. Le conseil de discipline régional appréciera s'il y a faute.

Le conseil de discipline régional se prononcera au sujet de la sanction proposée par le directeur.

En cas de litige, le conseil de prud'hommes intervient le cas échéant dans les conditions fixées par l'article L1333-1 et suivants du code du travail.

ARTICLE 15 : GARANTIE DES DROITS DES SALARIES

Conformément à la loi du 4 août 1982, aucune sanction ne peut être infligée au salarié sans que celui-ci soit informé dans le temps, et par écrit, des griefs retenus contre lui.

Préalablement à l'entretien, le salarié en cause doit recevoir communication des motifs de la décision envisagée et du dossier.

Quelle que soit la nature de la sanction, au cours de l'entretien, le salarié est entendu en présence des délégués du personnel. Il peut se faire assister par une personne de son choix appartenant au personnel de l'organisme pour assurer sa défense. De plus, l'employeur est tenu de recueillir les explications du salarié.

Dans les cas où la sanction disciplinaire entraîne la réunion du conseil de discipline régional, le salarié en cause peut, pour sa défense, être accompagné d'un conseiller de son choix.

Par ailleurs, le salarié doit recevoir communication de son dossier au moins huit jours avant la réunion du conseil de discipline régional.

Tout salarié qui en fait la demande peut consulter son dossier auprès de la Direction des ressources humaines, seul ou en présence d'un ou plusieurs délégués du personnel.

IV – SANTE, HYGIENE ET SECURITE

Toute personne présente dans les locaux de l'Urssaf Ile de France est tenue d'observer les mesures d'hygiène et de sécurité, les prescriptions du Service de santé au travail et les instructions de la Direction de la Gestion interne, même verbales.

Conformément aux instructions données par la Direction, il incombe à chaque salarié de prendre soin, en fonction de sa formation et selon ses possibilités, de sa sécurité, de sa santé, et de celles des autres personnes concernées par ses actes ou ses missions au travail.
Tout salarié qui constate ou qui a connaissance d'une défaillance ou d'une anomalie dans les installations ou le fonctionnement des machines, véhicules ou système de sécurité dont ila la charge doit en informer immédiatement son supérieur hiérarchique.

Tout accident, même bénin, survenu au cours du travail doit immédiatement être porté à la connaissance du supérieur hiérarchique et noté sur le registre des accidents bénins.

ARTICLE 16 : SANTE

16-1 En application des dispositions légales en vigueur, le personnel est tenu de se soumettre aux visites médicales obligatoires périodiques, aux visites médicales d'embauche

et de reprise, ainsi qu'aux visites prévues dans le cadre de la surveillance médicale renforcée.

Le refus du salarié de se soumettre aux obligations relatives à la santé peut entraîner l'une des sanctions prévues au présent règlement.

16-2 Les salariés doivent signaler à la Direction des ressources humaines le nom de la personne à prévenir en cas d'urgence ou le médecin qui doit être alerté.

16-3 Chaque site de l'organisme est équipé d'un défibrillateur cardiaque externe automatique qui peut être utilisé par tous pour faciliter la réanimation cardiaque. Son emplacement fait l'objet d'une signalétique appropriée. Sa maintenance est assurée régulièrement conformément à la législation en vigueur.

ARTICLE 17 : HYGIENE

17-1 Il est interdit de prendre ses repas dans les locaux affectés au travail.

17-2 Il est interdit de pénétrer ou de demeurer dans l'entreprise en état d'ébriété ou sous l'emprise de la drogue.

Nul ne peut introduire des boissons alcoolisées dans l'établissement, sauf autorisation exceptionnelle de la Direction.

L'organisation de réceptions dans les services, à l'occasion d'événements touchant la vie professionnelle (départs en retraite, etc.), doit faire l'objet d'une autorisation préalable.

17-3 En application de l'article L 3511-7 il est interdit de fumer dans tous les locaux de l'Urssaf Ile de France (parties communes, locaux collectifs ou locaux individuels), à l'exception des emplacements extérieurs réservés aux fumeurs sur chaque site de l'Urssaf Ile de France.

L'interdiction de fumer dans les locaux de l'Urssaf Ile de France s'entend également de la cigarette électronique.

17-4 Le personnel dispose d'armoires-vestiaires individuelles munies d'un système de fermeture.

Les armoires-vestiaires doivent être maintenues dans un état de propreté constante et il est interdit d'y conserver des denrées périssables ou des matières dangereuses.

Une désinfection partielle ou totale pourra être décidée par la direction de l'organisme.

En cas de nécessité liée à l'hygiène et à la sécurité, la direction sera en droit de faire ouvrir l'armoire, une fois le salarié informé, sauf urgence ou empêchement exceptionnel. Le salarié peut demander la présence d'un représentant du personnel.

En cas de risque grave et imminent pour la sécurité des personnes et des biens, la Direction peut être conduite à faire procéder à l'ouverture et à la vérification du contenu des vestiaires.

17-5 Dans l'hypothèse de l'émergence d'une épidémie, reconnue comme telle par les autorités sanitaires et emportant notamment l'obligation du port du masque en entreprise, les salariés amenés à travailler sur l'un des sites de l'organisme sont tenus de respecter cette consigne lors de leur présence dans un espace de travail clos et partagé, de même que lors de leurs déplacements dans les espaces de circulation ou parties communes (couloirs, toilettes, vestiaires, réfectoire, espaces de détente …).

17-6 Le refus du salarié de se soumettre aux obligations relatives à l'hygiène peut entraîner l'une des sanctions prévues au présent règlement.

ARTICLE 18 : SECURITE

18-1 Obligations générales

Le personnel assurant une mission nécessitant une présence permanente ou une astreinte pour surveiller le fonctionnement de machines et d'installations complexes ou assurant des missions d'hygiène et de sécurité ou de protection des personnes et des biens, ne peut quitter son poste de travail sans prévenir ou sans y être remplacé.

Chaque membre du personnel ou des entreprises intervenantes doit avoir pris connaissance des consignes de sécurité qui lui sont communiquées.

18-2 Accidents et maladies professionnelles

En cas d'accident de travail, une déclaration immédiate doit être faite au chef d'entreprise ou à ses représentants qualifiés –DRH-, soit par l'intéressé, soit par un témoin de l'accident.

De même, tout symptôme pouvant être considéré comme relevant d'une maladie professionnelle doit être signalé par l'intéressé au service de santé au travail.

18-3 Le refus du salarié de respecter ses obligations relatives à la sécurité peut entraîner l'une des sanctions prévues au présent règlement.

18-4 Evaluation et maîtrise des risques

L'inventaire des risques identifiés au sein des différents services de l'organisme, les résultats de leur évaluation ainsi que leurs moyens de maîtrise sont répertoriés dans un document unique. Il est mis à jour au moins une fois par an, ainsi que lors de toute décision d'aménagement important modifiant les conditions de travail ou de l'apparition de tout nouveau risque.

Le document est tenu à disposition des salariés de l'organisme, des membres du CHSCT, des délégués du personnel, du médecin du travail et des membres de l'inspection du travail. Un avis indiquant les modalités d'accès des salariés à ce document est affiché avec le présent règlement intérieur.

18-5 Participation des salariés à la continuité de l'activité de l'organisme

Un Plan de continuité d'activité (PCA) décrit le fonctionnement des services de l'Urssaf en mode dégradé ou en situation de crise majeure. L'ensemble du personnel est tenu de respecter les prescriptions du PCA qui fait l'objet d'une diffusion auprès de l'ensemble des salariés par le biais de l'intranet régional.

Le travail à distance peut être mis en œuvre en cas d'activation du PCA.

18-6 Protection des salariés

Tous les salariés de l'organisme ou des entreprises extérieures exerçant une activité professionnelle spécialisée et pour toutes spécialités (travaux, entretien, maintenance, conduite, manutention, sécurité générale), doivent respecter les consignes propres à la sécurité des personnes, en particulier, le port des accessoires ou dispositifs de signalisation ou de protection individuelle tels que ceintures ou baudriers de sécurité, casques, lunettes, bottes, chaussures, tenues de travail, vêtements imperméables ou résistants, gants, brassières, épaulières, tabliers, matériels isolants électriques, électrostatiques ou électroniques, qui ont été mis à disposition par l'organisme ou par les entreprises extérieures, lorsque sont exécutées des missions rendant obligatoire l'utilisation de ces moyens de signalisation ou de protection.

Les locaux techniques, les salles de machines génératrices ou machines motrices ne sont accessibles qu'au personnel affecté à la conduite et à l'entretien des installations et des machines.

Il est interdit de modifier ou de déplacer tous dispositifs de protection placés sur desmachines ou dans des locaux techniques. Cette même interdiction vise les outillages fixesou portatifs, les échelles, échafaudages et lieux d'intervention préparés à cet effet.

Il est rappelé que le travail sur des machines ou matériels techniques en mouvement exige des vêtements de travail ajustés et non flottants.

Tout conducteur de machines ou de matériels techniques doit respecter les consignes d'utilisation et de sécurité qui leur sont particulières.

Tout salarié qui, pour l'exercice de sa mission, utilise des outillages fixes ou portatifs, électriques, mécaniques, pneumatiques ou similaires, doit impérativement respecter les consignes d'utilisation.

Il est interdit aux salariés de l'organisme ou des entreprises extérieures de modifier les équipements de sécurité qui sont mis en place dans tous les domaines.

Les salariés de l'organisme, affectés dans les services spécialisés, à caractère technique et de sécurité, doivent porter, lorsque la mission l'exige, une tenue distinctive, un badge, un brassard ou une combinaison de travail. Cette obligation est applicable notamment aux salariés chargés des missions de maintenance et d'entretien.
Le personnel exposé à des risques spécifiques doit porter les équipements de protection individuelle adaptés (masque, chaussures de sécurité, casques, bouchons d'oreilles, lunettes, …) qui lui ont été prescrits et fournis.

18-7 Protection des travailleurs dans les établissements qui mettent en œuvre des courants électriques

Il est interdit, à toute personne non habilitée au sens de la norme NF.C 18 510, d'intervenir sur les installations électriques.

Toute personne dûment habilitée doit respecter, intégralement, la réglementation du décret du 14 novembre 1988 et ses annexes, les consignes particulières propres au service, les normes spécifiques et les règles de l'art en usage dans les professions intéressées.

18-8 Consignes particulières pour le stockage et l'utilisation des produits, substances ou préparations pouvant présenter des risques pour les personnes

Tous les produits identifiés comme : Toxiques, Nocifs, Corrosifs, ainsi que tous produits CMR (Cancérogène, Mutagène, Reprotoxique), dans la mesure où ils n'ont pu être remplacés par des produits non dangereux ou moins dangereux, doivent faire l'objet de l'accord des services techniques compétents pour toute utilisation, après consultation par ce dernier du Service de santé au travail.

La mise en place des fiches de données de sécurité sur le lieu de leur utilisation est obligatoire.

18-9 Prévention des incendies

Aucun salarié n'est autorisé à introduire, dans l'immeuble, des matières et liquides inflammables ou pouvant présenter des risques, sauf accord du secteur prévention et sécurité, et seulement pour les besoins du service.

Tout utilisateur de matières ou liquides inflammables, ou pouvant présenter des risques, doit se conformer strictement aux consignes d'utilisation qui leur sont propres, ainsi qu'aux dispositions des fiches de données de sécurité.

Il est interdit d'encombrer les circulations, les issues, les dégagements et les dispositifs de sécurité.

Les consignes, en cas d'incendie ou de sinistre, doivent être strictement respectées. Chaque salarié est tenu de participer aux exercices d'évacuation et aux séances d'information et de recyclage en matière de sécurité, incendie et risques divers.

18-10 Respect du règlement intérieur par les entreprises extérieures

Les entreprises extérieures sont tenues de respecter les clauses du décret n° 92-158 du 20 février 1992 fixant les prescriptions particulières d'hygiène et de sécurité applicable aux travaux et interventions effectués dans un établissement par une entreprise extérieure.

Le personnel des entreprises extérieures est tenu de respecter toutes les prescriptions d'hygiène et de sécurité de l'organisme et les règles posées par les services techniques compétents, et les engagements contractuels.
Les salariés des entreprises extérieures doivent porter, lorsque la mission l'exige, une tenue distinctive, un badge, un brassard ou une combinaison de travail.

Cette obligation est définie dans les engagements contractuels en matière de sécurité générale, sécurité d'incendie, maintenance et travaux spécialisés.

18-11 Sécurité des biens personnels des salariés

Afin de se prémunir contre les vols de biens personnels (sacs, vêtements, ...) les précautions nécessaires doivent être prises par leur propriétaire, notamment en ce qui concerne la fermeture des vestiaires et des véhicules garés dans les parcs de stationnement.

ARTICLE 19 : MODALITES D'EXERCICE DU DROIT D'ALERTE ET DE RETRAIT

Tout salarié ayant un motif raisonnable de penser qu'une situation de travail présente un danger grave et imminent pour sa vie ou sa santé peut se retirer de son poste comme la loi lui en donne le droit (articles L 4131-1 et L 4131-3 du Code du Travail).

Aucune sanction, aucune retenue de salaire ne peut être prise à l'encontre d'un salarié ou d'un groupe de salariés dans une telle situation.

ARTICLE 20 : CONDUITE DES VEHICULES

Les utilisateurs de véhicules terrestres à moteur qui disposent d'une autorisation de circuler pour les besoins du service doivent s'attacher au respect des règles du code de la route.

Les agents qui utilisent leur véhicule personnel dans le cadre de leurs activités professionnelles doivent attester chaque semestre de la validité de leur permis de conduire et de la conformité du certificat technique de leur véhicule à la réglementation, notamment en ce qui concerne les défauts obligatoirement soumis à réparation.

Les chauffeurs quant à eux doivent attester chaque semestre de la validité de leur permis de conduire.
Tout agent détenteur d'une autorisation de circuler et qui perd la validité de son permis de conduire doit le signaler obligatoirement à sa hiérarchie qui en avise immédiatement le service compétent.

L'utilisation du téléphone portable durant la conduite automobile et dans le cadre des actions liées aux missions est totalement interdite.

V – ENTREE EN VIGUEUR ET MODIFICATION DU REGLEMENT

ARTICLE 21 : DATE D'ENTREE EN VIGUEUR

Conformément à l'article L1321-4 du Code du travail, ce règlement a été soumis à l'avis du Comité social et économique et les formalités de communication et de dépôt auprès de l'inspecteur du travail et du conseil de Prud'hommes de Bobigny ont été effectuées.

Ce règlement entre en vigueur le 12 mai 2023 et fait l'objet d'un affichage conformément aux dispositions du Code du travail.

.

ARTICLE 22 : MODIFICATIONS ULTERIEURES

Toute modification ultérieure de ce règlement sera soumise à la même procédure, conformément au Code du travail.

Urssaf
Île-de-France

ANNEXE

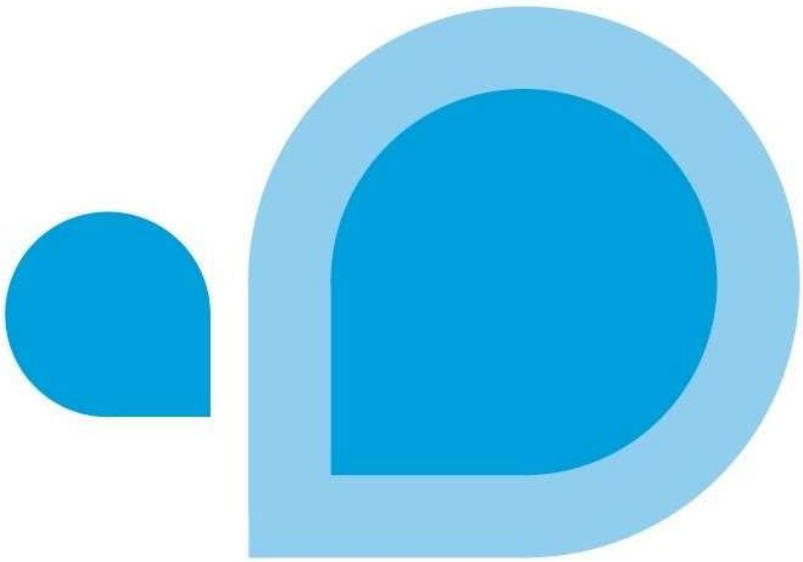
CHARTE INFORMATIQUE

DE L'URSSAF ILE-DE-FRANCE

Urssaf
Île-de-France

CHARTE UTILISATEUR

2022 - V4.0



Sécurité du SI

Fiche de gestion du document

HISTORIQUE DES MODIFICATIONS

Version	Crée ou modifié le	Rédacteur	Nature des mises à jour et commentaires
1.0	02/01/08	MOA SSI	Version initiale
2.0	22/11/12	MOA SSI	Version mise à jour (ajout parties « administrateurs », « réseaux sociaux », « utilisation d'outils personnels », …)
2.1	27/03/15	MOA SSI	Révision mineure annuelle (les révisions sont marquées en jaune) L'application du modèle 2015 n'est applicable qu'à l'occasion d'une nouvelle signature de charte (nouveaux entrants)
2.2	13/10/16	MOA SSI	Révision mineure annuelle (les révisions sont marquées en jaune) L'application du modèle 2016 n'est applicable qu'à l'occasion d'une nouvelle signature de charte (nouveaux entrants)
3.0	13/06/2019	MOA SSI	Version mise à jour (prise en compte RGPD, Cloud, contrôle…) Validée au COPIL SSI le 12/09/2019
3.1	04/02/2020	MOA SSI	Modifications substantielles sur aspects juridiques avec validation SDAJ le 23/01/2020 Validation par le Copil SSI Acoss le 04/02/2020
4.0	01/09/2022	SDSNUM	Modifications liées au télétravail, prise en compte d'évolutions légales et jurisprudentielles, Rapprochement d'article pour mise en cohérence d'articles, précisions apportées concernant l'application de la charte aux prestataires organisme. Validation SDSNUM le 18/05/2022 Validation SDAJ le 13/07/2022

TABLE DES MATIERES

PRÉAMBULE 5

Article 1 - Objectifs 5

Article 2 - Champ d'application 5

MISE À DISPOSITION DES RESSOURCES 6

Article 3 - Généralités 6

Article 4 - Disponibilité des ressources 7

Article 5 - Intégrité des données 7

Article 6 - Confidentialité des données 7

RÈGLES D'UTILISATION 8

Article 7 - Règles générales 8

Article 8 - Utilisation non professionnelle 9

Article 9 - Protection des ressources 9

Article 10 - Accès au SI en local 10

Article 11 - Accès au SI à distance 10

Article 12 - Accès logique et habilitations 10

Article 13 - Communication électronique 11

Article 14 – Informatique dans le cloud 12

Article 15 – Droits d'auteur, utilisation de code source 12

Article 16 - Sauvegarde de l'information 12

Article 17 - gestion des incidents 12

Article 18 - Gestion des départs 13

SPECIFICITES COMPLEMENTAIRES AUX ADMINISTRATEURS INFORMATIQUES ET PERSONNES HABILITEES 13

Article 19 - Maintenance et assistance 13

Article 20 - Objectifs 13

Article 21 - Intégrité des données 13

Article 22 - Confidentialité des données 14

Article 23 - Accès sur les postes de travail pour des opérations de maintenance, d'assistance 14

Article 24 - Respect de la propriété intellectuelle 14

Article 25 - Utilisation des comptes d'administration et d'exploitation 14

Article 26 - Responsabilité individuelle 15

MODALITÉS DE SUIVI 15

Article 27 - Mesures de contrôle 15

Article 28 - Conservation des traces d'accès 16

Article 29 - Non-respect de la charte 16

MODALITÉS D'APPLICATION 16

Article 30 - Valeur de la charte 16

Article 31 - Entrée en vigueur 16

PRÉAMBULE

ARTICLE 1 - OBJECTIFS

L'utilisation des ressources informatiques et de communication électronique suppose le respect de règles destinées à assurer un niveau optimum de sécurité, de confidentialité, de performance et d'une manière générale le respect des dispositions légales et réglementaires applicables.

Les principales règles de droit à respecter sont relatives au respect de l'intimité de la vie privée d'autrui, à la protection du secret des correspondances et du secret professionnel, à la protection de la propriété intellectuelle et des droits de la personne résultant des fichiers ou des traitements informatiques.

La présente charte tient compte des recommandations de la Commission Nationale de l'Informatique et des Libertés (Cnil).

Elle est rédigée dans l'intérêt de chaque utilisateur et manifeste la volonté de l'organisme d'assurer un accès et une utilisation sécurisés des ressources informatiques et de communication électronique.

La présente charte s'inscrit dans le cadre de la Politique Nationale de Sécurité du Système d'Information de la branche Recouvrement. Elle a pour objectif de formaliser les règles déontologiques et de sécurité que les utilisateurs et l'organisme s'engagent à respecter.

ARTICLE 2 - CHAMP D'APPLICATION

La présente charte qui a valeur de règlement intérieur, est applicable à l'ensemble des utilisateurs sans distinction (y compris les administrateurs informatiques et / ou personnes habilitées).

Est considérée comme « *utilisateur* » toute personne autorisée à accéder ou à employer les ressources informatiques et communication électronique, quel que soit son statut (salarié, personnel intérimaire, stagiaire, personnel des prestataires extérieurs, consultant, …).

Est considéré comme « *administrateur informatique* » tout utilisateur qui au titre de son activité professionnelle a pour mission d'assurer le bon fonctionnement et la sécurité des ressources du Système d'Information (SI) placées sous sa responsabilité (serveurs, équipements réseaux, équipements de sécurité, applications, bases de données, postes de travail, ...). Dans le cadre de sa mission, cet administrateur a des droits d'accès privilégiés aux outils bureautiques, applicatifs, infrastructures, systèmes et réseaux.

Est considérée comme « *personne habilitée* » toute personne (gestionnaire / expert fonctionnel ou technique, développeur, responsable de la sécurité du système d'information, …) auquel l'organisme a confié une mission particulière liée à la gestion d'une partie du SI (téléchargement et installation de logiciels, installation des infrastructures et postes de travail, administration d'une ou plusieurs bases de données, assistance fonctionnelle ou technique, …).

La présente charte peut être complétée, le cas échéant, de documents spécifiques pour certaines catégories de personnel.

Sont considérées comme « *ressources informatiques et communication électronique* » et/ou « système d'information », l'ensemble des architectures techniques, les applications, les moyens de communication électronique et les données. Ces ressources comprennent notamment la messagerie électronique permettant l'échange de courriers et de documents, les sites mis à disposition par Intranet et / ou Internet, les postes de travail, les smartphones, le cloud professionnel (par exemple Office 365) ainsi que les applications et données mise à disposition par nos partenaires nécessitant une habilitation.

Conformément aux dispositions de l'article L.1222-9 du Code du travail, « le télétravail désigne toute forme d'organisation du travail dans laquelle un travail qui aurait également pu être exécuté dans les locaux de l'employeur est effectué par un salarié hors de ces locaux de façon volontaire en utilisant les technologies de l'information et de la communication ».

Tous les salariés se trouvant en dehors de leur organisme de rattachement, qu'ils soient en télétravail (en application de l'article sus visé du code du travail) ou pas doivent faire preuve d'une vigilance accrue en matière de confidentialité et de protection des données notamment lorsqu'ils se trouvent à proximité de personnes sans lien avec leurs activités professionnelles et sont visés par la présente charte.

MISE À DISPOSITION DES RESSOURCES

ARTICLE 3 - GENERALITES

Les ressources informatiques et de communication électronique peuvent être mises à la disposition de l'utilisateur dans l'exercice de son activité professionnelle. Elles sont et demeurent la propriété de l'organisme ou du prestataire de services avec qui l'organisme a conclu un contrat pour ce faire.

Les équipements et services mis à la disposition de l'utilisateur sont exclusivement installés, configurés et paramétrés par le personnel habilité par la direction. L'utilisateur s'interdit de modifier les équipements mis à sa disposition par l'ajout de logiciels ou de matériels pour quelque raison que ce soit. Si ces logiciels ou matériels lui semblent nécessaires pour l'exercice de sa mission, il en fait part à sa hiérarchie ou s'il s'agit d'un externe à l'organisme, à son donneur d'ordre.

L'utilisateur s'engage à ne pas modifier les configurations d'accès des administrateurs informatiques à son poste travail. A des fins de précaution, certaines configurations peuvent être verrouillées par l'organisme (poste de travail, accès à Internet, …).

L'utilisateur a la responsabilité des ressources informatiques et de communication électronique qui lui sont confiées. Il ne doit ni les prêter, ni divulguer leur mode de fonctionnement et doit signaler immédiatement à sa hiérarchie ou à son donneur d'ordre leur disparition ou leur détérioration.

L'utilisation des ressources informatiques et de communication électronique suppose :

- le respect des dispositions légales et réglementaires applicables,
- la compréhension et le respect de règles destinées à assurer le meilleur compromis entre facilité, confort d'utilisation et disponibilité d'une part, intégrité et confidentialité d'autre part.

ARTICLE 4 - DISPONIBILITE DES RESSOURCES

L'utilisateur est averti de l'existence de règles de gestion des ressources informatiques et de communication électronique. L'organisme peut interrompre, modifier ou supprimer tout ou partie des équipements et des services pour quelque raison que ce soit, de manière temporaire ou définitive et non discriminatoire.

L'organisme s'efforcera, autant que faire se peut, de prévenir les utilisateurs dans des délais raisonnables, notamment en cas de maintenance.

L'utilisateur ne doit pas entraver la continuité de service, conformément aux modalités d'organisation du service et à celles définies par la hiérarchie ou le donneur d'ordre pour les externes.

ARTICLE 5 - INTEGRITE DES DONNEES

L'utilisateur s'engage à ne pas porter atteinte à l'intégrité et à la conservation des données de l'organisme en respectant les finalités des outils mis à sa disposition.

Il s'interdit de charger ou de transmettre sciemment des fichiers contenant des virus ou des données altérées.

Les règles spécifiques découlant des missions des administrateurs informatiques ou des personnes habilitées sont détaillées à l'article 21.

ARTICLE 6 - CONFIDENTIALITE DES DONNEES

Les informations émises, reçues et stockées par l'utilisateur à l'aide des ressources informatiques et de communication électronique, concourent à l'exercice de sa mission professionnelle au sein de la branche Recouvrement. Dans le respect des règles de confidentialité des données, l'utilisateur limite ses accès aux ressources informatiques liées à la finalité de sa mission professionnelle. Il ne peut donc, sans autorisation expresse de sa hiérarchie, utiliser des données auxquelles il aurait accès dans le cadre de ses fonctions professionnelles et en aucun cas à des fins personnelles. Il doit être particulièrement vigilant vis-à-vis des données qu'il extrait du système d'information.

La confidentialité des données, dont le Recouvrement est dépositaire, est garantie par l'obligation de secret professionnel.

L'accès aux applications et aux données du système d'information est strictement réservé à ce qui est rendu nécessaire par l'exercice professionnel. L'autorisation d'accès est formalisée par l'obtention d'une habilitation validée par le directeur et le directeur comptable et financier. Tout agent disposant d'une habilitation reste soumis :

- aux règles déontologiques quant à l'accès à l'information
- au secret professionnel quant aux règles de communication de ces informations.

A ce titre, il doit s'assurer avant de communiquer des données professionnelles que les destinataires sont dûment habilitées à en connaitre.

Pour garantir la confidentialité de ces données professionnelles, leurs transmissions à l'aide des ressources informatiques et de communication électronique ne peuvent être réalisées qu'aux conditions suivantes :

- habilitation de l'émetteur,
- désignation d'un destinataire autorisé,
- respect d'une procédure sécurisée, formalisée et validée par l'organisme de l'émetteur et par celui du destinataire.

La confidentialité des données du Recouvrement ne peut être garantie sur des messageries électroniques personnelles. Le transfert de données professionnelles sur les messageries électroniques personnelles des agents du Recouvrement est donc proscrit. Le stockage de données professionnelles est également interdit sur des ressources privées tant sur supports physiques que sur Internet.

L'ensemble de ces données sont et demeurent la propriété de l'organisme, à l'exception de celles résultant de l'activité des instances représentatives du personnel et de celles prévues par le présent document (*Cf. article 8*).

Les règles spécifiques découlant des missions des administrateurs informatiques ou des personnes habilitées sont détaillées à l'article 22.

RÈGLES D'UTILISATION

ARTICLE 7 - REGLES GENERALES

Les conditions d'utilisation des ressources informatiques et de communication électronique sont définies par l'autorité hiérarchique ou le donneur d'ordre pour les externes, qui se réserve notamment le droit de restreindre ou de filtrer les accès et usages.

L'utilisateur est responsable du bon usage des ressources informatiques et de communication électronique et s'engage à les utiliser dans le respect :

- des lois relatives à la propriété intellectuelle en ne faisant pas de copies illicites des logiciels commerciaux ou du Recouvrement,
- des lois relatives aux droits d'auteur (fichiers multimédias, …),
- la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée,
- le règlement n°2016/679/UE dit « général sur la protection des données »,
- des lois relatives aux publications portant atteinte à la dignité de la personne humaine,
- des procédures et méthodologies qui lui sont adressées (notes de direction, procédures, manuels utilisateurs, …).

Il ne doit pas employer les ressources informatiques et de communication électronique à des fins de harcèlement, de menace, ni publier ou distribuer des informations à caractère promotionnel ou lucratif.

L'utilisateur est également tenu par un devoir de réserve et de loyauté envers son employeur lorsqu'il communique publiquement dans un cadre professionnel ou privé.

L'utilisateur ne doit en aucune manière se livrer à la consultation, au chargement, au stockage, à la publication ou à la diffusion de fichiers et de messages dont le contenu :

- présente un caractère injurieux, raciste, pornographique ou diffamatoire, et de manière générale illicite,
- porte atteinte à l'intégrité et à la conservation des données de l'organisme,
- porte atteinte à la déontologie professionnelle, à l'image de marque interne et externe de l'organisme ou de l'institution.

Cette liste n'est pas exhaustive. Ceci s'applique tant aux fichiers qu'aux messages, avec ou sans pièces attachées, quelle que soit la forme des contenus (sonores, audiovisuels, multimédias ou logiciels).

Il doit proscrire tout comportement pouvant inciter des tiers à lui adresser de tels documents et les détruire en cas de réception fortuite.

La création de tout fichier contenant des informations permettant l'identification d'une personne physique, doit faire l'objet d'une autorisation préalable de sa hiérarchie de façon à respecter le RGPD (Règlement Général sur la Protection des Données). La collecte abusive et/ou déloyale, l'accès illégitime, la divulgation ou le détournement des informations sont interdits. Les personnes concernées doivent être informées préalablement de la constitution du fichier.
Pour tout nouveau traitement de données à caractère personnel, le DPO (Délégué à la protection des données) doit être obligatoirement sollicité.

Une attention toute particulière est à apporter sur les zones de commentaires ou de saisies libres que les utilisateurs peuvent être amenés à compléter dans l'exercice de leurs missions. En effet, les informations ainsi renseignées ne doivent pas être excessives au regard des objectifs poursuivis par le traitement, ni a fortiori interdites.

ARTICLE 8 - UTILISATION NON PROFESSIONNELLE

L'utilisation des ressources informatiques et de communication électronique à des fins non professionnelles est tolérée pour répondre à des obligations socialement admises. Cette utilisation doit demeurer raisonnable. En tout état de cause, l'utilisation des ressources informatiques et de communication électronique à des fins non professionnelles ne doit pas avoir pour effet de nuire à la qualité du travail ni au temps qui est consacré à celui-ci. Un tel usage ne doit pas perturber le bon fonctionnement du système d'information.

Les messages sont en tout état de cause émis et reçus sous la seule responsabilité de l'utilisateur. La confidentialité attachée à la correspondance non professionnelle implique la mention du terme « privé » dans la zone « objet » du message. La perspective d'une réponse impose d'informer le tiers destinataire de cet usage. Le recours aux pièces jointes est à éviter.

L'utilisateur s'engage à ne pas qualifier de « privé » un message professionnel.

L'employeur se réserve le droit de limiter ou de suspendre cette tolérance en cas d'abus.

Il est possible de créer un répertoire privé au sein du disque dur de l'ordinateur ou dans son espace cloud professionnel sous réserve qu'il soit identifié sous le terme « privé ».

L'utilisateur s'engage à ne pas stocker de données professionnelles sous un répertoire identifié « privé ».

L'organisme employeur n'a aucune obligation quant à la réalisation de sauvegardes concernant les messages et fichiers dits « privés ».

Les règles d'accès aux messages et répertoires privés sont traitées :

- *dans le cadre de la maintenance aux articles 16, 22 et 23;*
- *dans le cadre des contrôles de sécurité à l'article 27.*

ARTICLE 9 - PROTECTION DES RESSOURCES

Les postes de travail sont configurés et protégés afin de pouvoir détecter ou résister à différents incidents (virus, logiciels espions, failles de sécurité, …). Seules les personnes habilitées sont autorisées à installer des logiciels sur ces postes.

Les protections mises en place (anti-virus, pare-feu, chiffrement, …) reposent sur des outils qui s'exécutent et se mettent à jour périodiquement. Pour des raisons de sécurité, un déchiffrement des données peut être réalisé par l'employeur. L'utilisateur ne doit pas tenter de désactiver ces outils de protection ou entraver leur fonctionnement et s'engage à signaler toute anomalie.

L'utilisateur doit suivre la procédure en vigueur dans l'organisme avant d'utiliser un support de données amovible (clé USB, smartphone, …).

Tout équipement connecté à un outil informatique mis à la disposition de l'utilisateur par l'organisme (Smartphone, clé USB, …) étant présumé utilisé à des fins professionnelles, l'organisme peut, par le biais d'outils de sécurité ou de personnes habilitées, avoir accès à des fichiers non identifiés comme personnels sur l'équipement connecté, hors la présence du salarié.

L'utilisateur est informé des conséquences résultant des divers outils de contrôle et d'analyse, à savoir le retardement, le blocage ou la suppression de messages présentant des risques liés à leur taille ou à leur contenu, ou encore le non-acheminement d'un message jugé non légitime.

Lorsqu'un utilisateur est doté d'équipements mobiles, il en assure la garde et la responsabilité en tous lieux. Il avertit l'organisme et, selon les cas, procède lui-même à toutes les démarches (déclaration d'assurance, dépôt de plainte, …) rendues nécessaires à la suite d'un incident.

ARTICLE 10 - ACCES AU SI EN LOCAL

Seules les personnes habilitées par l'organisme peuvent connecter ou déconnecter des équipements informatiques sur le réseau de l'organisme.

L'utilisateur s'engage à :

- Ne pas effectuer d'opérations qui pourraient avoir pour conséquence d'interrompre ou de dégrader le fonctionnement du réseau ou d'un système connecté,
- Ne pas connecter au réseau du Recouvrement de matériels informatiques non maitrisés par le Recouvrement (ordinateur portable tablette ou smartphone personnel, d'un prestataire, …).

ARTICLE 11 - ACCES AU SI A DISTANCE

L'accès à distance au système d'information du Recouvrement est autorisé aux personnes habilitées à partir de postes de travail « maîtrisés » ou « non maîtrisés ». Les postes « maîtrisés » sont les postes configurés, sécurisés et mis à disposition par le Recouvrement aux salariés avec engagement à ne pas en modifier la configuration. Les postes « non maîtrisés » ne sont pas configurés par le Recouvrement (poste personnel, partenaire, hôtel, …)

Ces accès doivent respecter la politique nationale de sécurité de « gestion des accès distants ».

Lorsqu'un accès à distance est accordé à un utilisateur, celui-ci s'engage à employer les moyens techniques d'authentification qui lui seront remis et aucun autre. En termes de sécurité et de confidentialité, l'utilisateur est soumis aux mêmes obligations et règles que celles établies dans l'article 12 visées et devra suivre toutes les prescriptions complémentaires qui lui seront signifiées. Il devra aviser sans délai les services compétents de la perte ou du vol du moyen d'authentification à distance.

L'emploi des ressources informatiques et de communication électronique nomades impose à l'utilisateur un niveau de surveillance et de confidentialité renforcé.

L'utilisateur de ces équipements doit notamment :

- s'informer des procédures de mise à jour de son poste de travail et les respecter,
- veiller à ce que des tiers non autorisés ne puissent ni accéder ni utiliser ces moyens, les éléments accessoires et leurs contenus.

ARTICLE 12 - ACCES LOGIQUE ET HABILITATIONS

Conformément à ses habilitations, chaque utilisateur accède aux ressources informatiques et de communication électronique après identification et authentification au système d'information.

Les identifiants sont personnels. Les authentifiants sont personnels et confidentiels.

Tout usage des ressources informatiques et de communication électronique est réputé avoir été réalisé par le porteur de l'identifiant d'accès. Il en assume alors les conséquences juridiques et financières, sauf :

- défaut avéré du système d'information ou de ses dispositifs de sécurité,
- si une demande de suppression ou de suspension de ses habilitations a été préalablement engagée, conformément à la procédure en vigueur,
- si la preuve d'usurpation de son identifiant peut être apportée.

En conséquence, l'utilisateur s'engage à :

- ne pas communiquer ses authentifiants,
- ne pas utiliser d'identifiants et d'authentifiants autres que les siens,
- appliquer les modalités de gestion des mots de passe (longueur, complexité, fréquence de modification, …),
- ne pas tenter d'accéder au système d'information par des moyens illicites (usurpation ou masquage d'identité, utilisation ou développement d'outils ne respectant pas les habilitations accordées, …),
- informer le propriétaire légitime de tout authentifiant dont il aurait eu connaissance, afin qu'il puisse procéder à son changement,
- ne pas employer les mots de passe utilisés pour l'accès aux ressources informatiques du Recouvrement (organisme, inter-région ou branche) sur d'autres systèmes, comme les sites Internet, …
- ne pas se servir des mêmes mots de passe que ceux qu'il utilise dans sa vie privée.

Les utilisateurs de comptes techniques partagés s'engagent à suivre strictement les procédures spécifiques mises en œuvre comprenant les modalités de partage et de changement des mots de passe.

Le poste de travail (ou tout autre équipement informatique) doit être verrouillé par l'utilisateur, dès qu'il s'absente, pour éviter toute utilisation par une tierce personne.

ARTICLE 13 - COMMUNICATION ELECTRONIQUE

Les messages électroniques sont émis sous la seule responsabilité de l'utilisateur. Le contenu de ces échanges pouvant engager juridiquement l'organisme, l'utilisateur doit, être vigilant sur la nature des messages qu'il envoie ou qu'il échange.

Le transfert, automatique ou manuel, de messages électroniques professionnels sur une messagerie électronique personnelle est interdit (*Cf. article 6*).

A des fins de non-saturation des ressources, les règles de gestion de la messagerie autorisent le retardement, l'interdiction d'envoi ou encore la suppression de fichiers présentant des risques liés à leur taille ou à leur contenu. Ces règles supposent notamment :

- la vigilance dans l'envoi de pièces jointes (en taille et en nombre),
- l'utilisation d'outils de compression pour les pièces jointes,
- l'interdiction de propager des messages de type « boule de neige » ou « chaîne » (dont la principale caractéristique est de demander de faire suivre le message) et l'obligation de les supprimer,
- la prudence quant à la communication de son adresse de messagerie professionnelle à des lettres d'information, sites et forums, pour éviter de recevoir des messages non sollicités.

Dans l'hypothèse où l'utilisateur recevrait, régulièrement ou non, des messages non sollicités ou qui seraient manifestement illicites, il préviendra immédiatement sa hiérarchie ou son donneur d'ordre pour les externes afin qu'elle puisse prendre les mesures nécessaires en fonction des obligations légales, de ses possibilités techniques et de ses contraintes économiques.

Chaque utilisateur doit organiser et mettre en œuvre, selon les instructions de sa hiérarchie ou de son donneur d'ordre, les moyens nécessaires à la conservation des messages, lorsque cela est nécessaire.

Pour la navigation internet, les outils de sécurité mettent en œuvre des moyens d'analyse et d'accès à des sites ou des pages dont les contenus ne correspondent pas aux missions du Recouvrement ou présentent des risques pour l'organisme.

ARTICLE 14 – INFORMATIQUE DANS LE CLOUD

Des environnements de travail collaboratif de type « Cloud Computing » (Informatique en nuage) sont mis à disposition des collaborateurs, dans le cadre d'un usage professionnel (réseaux sociaux d'entreprise, stockage/partage, messagerie, outils collaboratifs…) afin d'améliorer l'organisation, la mobilité ainsi que les conditions de travail en groupe.

Chaque utilisateur doit adopter un comportement responsable vis-à-vis du système d'information du Recouvrement en portant notamment une attention particulière en ce qui concerne le stockage et le transfert vers le cloud de données soumises à des règles de confidentialité (Cf. article 6) et de secret professionnel.

Avant de transmettre ou partager des données via le cloud ou la messagerie, il doit s'assurer que l'ensemble des destinataires sont dûment habilités à en connaitre.

ARTICLE 15 – DROITS D'AUTEUR, UTILISATION DE CODE SOURCE

Chaque agent est responsable des données qu'il utilise dans le cadre de la création de ses documents (bureautique, application, code source, logiciel, base de données, photographie…). A ce titre il ne peut utiliser, exploiter, copier, télécharger tout ou partie des données mises à disposition, publiées par un tiers et protégées par le droit d'auteur. En cas d'utilisation, l'agent doit s'assurer d'obtenir l'autorisation préalable de l'ayant droit.

En cas d'utilisation et/ou de développement réalisé à partir de code sous licence Open Source, l'utilisateur doit s'assurer que :

- le recours à cette licence est conforme à la stratégie du Recouvrement et respecte les procédures internes en vigueur en matière de développement open source et d'open innovation ;
- les conditions de cette licence sont compatibles avec le projet poursuivi, notamment en raison de ses potentiels effets « contaminants ».

ARTICLE 16 - SAUVEGARDE DE L'INFORMATION

Les utilisateurs sont tenus d'enregistrer les données professionnelles qu'ils manipulent sur des serveurs ou des répertoires sauvegardés dans le cadre des procédures en vigueur dans l'organisme.

Les utilisateurs doivent être conscients que :

- les sauvegardes ne permettent pas de récupérer des données au-delà d'une certaine ancienneté,
- seules les données sauvegardées pourront être restaurées en cas de perte.

ARTICLE 17 - GESTION DES INCIDENTS

L'utilisateur est tenu d'informer sans délai sa hiérarchie ou son donneur d'ordre pour les externes en cas de dysfonctionnement, anomalie, altération, perte, vol, destruction et de tout autre événement pouvant affecter les ressources informatiques et de communication électronique qu'il utilise.

Dans le cas où l'utilisateur serait invité à prendre des mesures d'urgence ou de sécurité spécifique, celui-ci s'engage à les appliquer sans le moindre délai.

L'administrateur informatique et / ou la personne habilitée conservera une trace des incidents de sécurité, survenue dans son périmètre d'activité, selon les modalités prévues dans la politique sécurité de l'organisme et dans la limite de la législation en vigueur.

ARTICLE 18 - GESTION DES DEPARTS

Lors de son départ de l'organisme, l'utilisateur doit remettre à sa hiérarchie ou s'il s'agit d'un externe à l'organisme, à son donneur d'ordre, les ressources informatiques et de communication électronique qui lui ont été remises (ordinateurs, périphériques, mobiles, PDA, carte d'accès, moyens d'authentification à distance, badges, supports de stockage, …) en bon état général de fonctionnement.
Le compte de messagerie et les habilitations de l'utilisateur sont supprimés à son départ conformément à la politique de sécurité.

Le répertoire « privé » doit être supprimé par l'utilisateur au plus tard la veille de son départ de l'organisme. En cas de décès ou de départ imprévu, l'organisme détruira dès qu'il en aura connaissance, toutes les données privées. A défaut, et sauf procédure judiciaire ou enquête administrative, ce répertoire est automatiquement supprimé le lendemain du départ sans être consulté et sans qu'aucune copie ne soit réalisée.

SPECIFICITES COMPLEMENTAIRES AUX ADMINISTRATEURS INFORMATIQUES ET PERSONNES HABILITEES

ARTICLE 19 - MAINTENANCE ET ASSISTANCE

La mise à disposition des ressources informatiques et de communication électronique implique nécessairement des opérations de maintenance technique et d'assistance aux utilisateurs.

Ces opérations de maintenance peuvent nécessiter l'intervention d'une « personne habilitée » sur site ou sous la forme d'une « prise de main à distance ». La « personne habilitée » est la personne désignée à cet effet par l'organisme (*Cf. article 2*).

L'objectif de ces opérations n'est autre que d'assurer le bon fonctionnement et la sécurité du système d'information. Cependant dans le cadre de ces interventions, la « personne habilitée » peut être amenée à prendre connaissance de messages émis ou reçus par l'utilisateur et à examiner en détail le journal de ses connexions.

La « personne habilitée » fera en sorte de ne pas accéder au répertoire intitulé « privé » et aux messages d'objet « privé », en dehors de la présence de l'utilisateur. Cependant elle peut y être contrainte pour des raisons de sécurité, pour des raisons techniques (surcharge du système, lutte anti-virus ou anti-spam, …) ou pour des raisons de continuité de service.

Les règles d'accès aux postes de travail pour des opérations de maintenance et d'assistance sont détaillées à l'article 23. Les règles pour les audits de sécurité sont détaillées à l'article 27.

ARTICLE 20 - OBJECTIFS

En complément des articles précédents, du fait de l'exercice de leurs missions et de leurs responsabilités, les administrateurs informatiques et les personnes habilitées ont des droits spécifiques quant à l'utilisation et la gestion de tout ou partie du SI (*Cf. article 2*). Ils sont soumis à des règles spécifiques et complémentaires (*Cf. articles 21 à 26*).

ARTICLE 21 - INTEGRITE DES DONNEES

L'administrateur informatique et / ou la personne habilitée s'engage à ne pas porter atteinte à l'intégrité du système d'information de l'organisme en respectant les finalités des outils mis à sa disposition.

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, d'exploitation ou de sécurité définies.

ARTICLE 22 - CONFIDENTIALITE DES DONNEES

L'administrateur informatique et / ou la personne habilitée est contraint à une obligation de confidentialité renforcée. Cette obligation de confidentialité renforcée porte sur l'ensemble des informations et données dont l'administrateur informatique et / ou la personne habilitée pourrait avoir connaissance dans le cadre de ses fonctions à l'exclusion des seules données publiques.

Il ne peut fournir un accès à des ressources privées (fichiers, messageries électroniques…) d'un collaborateur, y compris à sa hiérarchie ou pour les externes à son donneur d'ordre, sans le consentement écrit de cette personne, sauf cas exceptionnel et imprévu (décès, accident, …).

ARTICLE 23 - ACCES SUR LES POSTES DE TRAVAIL POUR DES OPERATIONS DE MAINTENANCE, D'ASSISTANCE

Plusieurs types de missions peuvent nécessiter l'intervention sur le poste d'un utilisateur, directement ou sous la forme d'une prise de contrôle à distance :

- les opérations de maintenance technique destinées à installer, configurer ou à garantir le bon fonctionnement des ressources informatiques mises à disposition de l'utilisateur,
- l'assistance technique ou fonctionnelle.

Dans le cadre de ces missions, les outils de prise de contrôle à distance sont installés sur le poste de travail et donnent un accès complet au système sur lequel il s'exécute.

En matière d'assistance sur les postes clients :

- les outils de prise de contrôle à distance doivent être configurés de manière à recueillir l'accord explicite de l'utilisateur avant toute intervention sur son poste si sa session est ouverte. Si aucune session n'est ouverte, l'administrateur informatique ou la personne habilitée peut directement prendre le contrôle de la machine.
- dans tous les cas, ces interventions doivent être tracées et l'utilisateur doit pouvoir constater si une prise en main à distance est en cours et quand elle se termine.

D'une manière générale et dans la mesure du possible, les administrateurs ont le devoir d'informer les utilisateurs de toute intervention nécessaire, susceptible de perturber ou d'interrompre la production.

ARTICLE 24 - RESPECT DE LA PROPRIETE INTELLECTUELLE

L'administrateur informatique ou la personne habilitée s'engage à respecter et à faire respecter la législation relative à la propriété intellectuelle. Pour cela, il informe toutes les personnes nécessaires et supprime si besoin les données qui contreviennent à cette législation.

Avant toute installation de logiciel l'administrateur informatique et / ou la personne habilitée doit s'assurer que l'organisme, le centre informatique ou le Recouvrement (dans le cas de licences nationales) dispose du nombre de licences nécessaires.

ARTICLE 25 - UTILISATION DES COMPTES D'ADMINISTRATION ET D'EXPLOITATION

Les utilisateurs de comptes d'exploitation et d'administration s'engagent à suivre strictement les procédures et modalités locales, interrégionales ou nationales en vigueur.

Etant donné que toute action sur le SI peut faire l'objet d'une journalisation permettant leur traçabilité, l'administrateur informatique et / ou la personne habilitée doit utiliser, sauf exception justifiée, son compte professionnel nominatif.

ARTICLE 26 - RESPONSABILITE INDIVIDUELLE

Lorsque l'administrateur constate des violations de la loi ou de la réglementation dans son périmètre d'activité, il en fait rapport à ses responsables hiérarchiques ou à ses donneurs d'ordre pour les externes, qui prendront les mesures adéquates afin de coordonner leurs actions avec les autorités judiciaires. Il peut prendre, après validation de sa hiérarchie ou de son donneur d'ordre, toutes les mesures conservatoires permettant de garantir la sécurité du Système d'Information et l'authenticité des preuves.

L'administrateur informatique et / ou la personne habilitée a le devoir de désobéir et d'alerter par écrit sa hiérarchie ou à son donneur d'ordre pour toute instruction qui aurait pour conséquence de lui faire commettre une infraction, que ce soit suite à la violation d'un droit fondamental de l'utilisateur, ou le non-respect d'une stipulation ou disposition décrite dans cette charte ou dans la loi. Toutefois cette alerte ne dégage pas l'administrateur de sa responsabilité.

L'administrateur informatique et / ou la personne habilitée doit connaître les règles de sécurité à respecter et sensibilise les utilisateurs aux problèmes de sécurité informatique. Il configure le système ou le réseau, développe les outils du Recouvrement, dans le sens d'une meilleure sécurité et conformément aux règles et politiques nationales.

L'administrateur informatique et / ou la personne habilitée ne peut être tenu responsable des données hébergées sur le système d'information en dehors de ses propres données.

MODALITÉS DE SUIVI

ARTICLE 27 - MESURES DE CONTROLE

Pour répondre aux obligations de l'organisme vis-à-vis des textes législatifs et règlementaires (ex : RGPD), de la politique de Sécurité du Recouvrement et de la présente charte, l'utilisation du SI et de l'accès aux données peut être soumis à des contrôles.

La direction de l'organisme peut diligenter toute opération de contrôle permettant de vérifier le respect de la présente charte ou des dispositions légales/règlementaires, soit de sa propre initiative, soit à l'initiative d'un tiers :

- Dans le cadre de procédures judiciaires,
- D'enquêtes administratives
- De demande du responsable de traitement des données.

Dans le cadre de ces opérations de contrôle, les personnes mandatées par la direction peuvent notamment être amenées à ouvrir tout message ou fichier non privé et à vérifier l'ensemble des connexions d'un utilisateur. Ces opérations de contrôles peuvent être réalisées sans l'accord de l'utilisateur.

Cependant, les fichiers identifiés comme privés pourront faire l'objet d'une mesure de contrôle, en présence du salarié ou lorsque celui-ci a été dûment appelé sauf risque ou évènement particulier.

Lors de ces contrôles, les personnes mandatées sont tenues de respecter la confidentialité des informations auxquelles elles accèdent.

Des règles spécifiques pour les administrateurs informatiques ou les personnes habilitées sont détaillées à l'article 26.

ARTICLE 28 - CONSERVATION DES TRACES D'ACCES

Les traces détaillées d'activité sont conservées pendant la durée légale, réglementaire ou conventionnelle, à l'issue de laquelle elles sont détruites. Elles sont considérées comme preuve de l'utilisation des ressources informatiques et de communication électronique par les utilisateurs. Elles peuvent faire l'objet d'un traitement statistique anonyme.

Ces traces peuvent être fournies aux personnes habilitées, aux services ressources humaines de l'organisme dans la limite de leurs besoins respectifs, aux autorités compétentes selon les dispositions légales et réglementaires en vigueur ; elles peuvent aussi être communiquées à l'utilisateur, pour les seules données qui le concerne directement et individuellement, en application des dispositions dites « Informatique et Libertés » et du règlement général sur la protection des données.

ARTICLE 29 - NON-RESPECT DE LA CHARTE

Le non-respect de tout ou partie des règles définies dans la présente charte peut entraîner pour l'utilisateur :

- le rappel des règles, voire la suspension ou la suppression de l'accès à certaines ressources informatiques.

- l'une des sanctions disciplinaires prévues au présent règlement et/ou des poursuites judiciaires.

Le non-respect de tout ou partie de la présente charte par les prestataires entraînera les conséquences prévues aux contrats encadrant lesdites prestations de services.

MODALITÉS D'APPLICATION

ARTICLE 30 - VALEUR DE LA CHARTE

La présente charte est annexée au règlement intérieur.

ARTICLE 31 - ENTREE EN VIGUEUR

Ayant été soumise pour avis au CSE le 5 avril 2023, la présente charte a été communiquée à l'Inspection du travail dont relève l'organisme, en deux exemplaires, et a fait l'objet d'un dépôt auprès du Greffe du Conseil des Prud'hommes.
Elle a été préalablement affichée conformément aux dispositions du Code du Travail.
Conformément aux dispositions légales, l'entrée en vigueur de la présente charte ne peut intervenir qu'à l'issue du délai d'un mois suivant l'accomplissement de l'intégralité des formalités de publicité et de dépôt précitées.
La date d'entrée en vigueur de la présente charte est fixée au *15 juin 2023* date à compter de laquelle elle se substitue, dans l'ensemble de ses stipulations, à la charte de même objet applicable au sein de l'organisme.