CAISSE D'EPARGNE
D'AUVERGNE ET DU LIMOUSIN

REGLEMENT INTERIEUR
- CAISSE D'EPARGNE ET DE PREVOYANCE D'AUVERGNE ET DU LIMOUSIN-

PREAMBULE

Article 1 : Objet et champ d'application

1.1. Objet

Conformément aux articles L 1321-1 et suivants du Code du travail, le Règlement Intérieur de l'entreprise fixe principalement les mesures d'application de la règlementation en matière de santé et de sécurité au sein de la Caisse d'Epargne et de Prévoyance d'Auvergne et du Limousin (*ci-après CEPAL*), les règles générales et permanentes relatives à la discipline et rappelle les garanties dont leur application est entourée.
Il intègre les dispositions conventionnelles applicables au sein du Groupe BPCE, de la Branche Caisse d'Epargne et de l'entreprise dans les domaines objets du présent règlement.

1.2. Champ d'application

Le présent Règlement s'applique, ainsi que ses annexes, à tous les salariés de l'entreprise, quels que soient la nature, la durée et le lieu d'exercice de leur emploi, sous réserve des dispositions législatives, réglementaires ou conventionnelles relatives à l'exercice du droit syndical et du mandat des représentants du personnel.

Il s'applique également à toute personne présente dans l'entreprise en qualité de stagiaire, d'intérimaire, de salarié d'entreprises extérieures intervenant, de façon permanente ou occasionnelle, à quelque titre que ce soit, et ce, en ce qui concerne les règles générales et permanentes relatives à la discipline, l'hygiène et la sécurité (à l'exclusion des dispositions relatives aux sanctions et à la procédure disciplinaire).

La hiérarchie est fondée à veiller à l'application du Règlement Intérieur.

1.3. Dispositions spéciales et modifications du règlement intérieur

Des dispositions spéciales pourront être prévues, en raison des nécessités de services, pour certaines catégories de salariés par exemple, mais aussi d'une manière plus générale en fonction de l'évolution des dispositions réglementaires ; elles feront l'objet de notes de services, ou procédures établies dans les mêmes conditions que le présent Règlement dans la mesure où elles portent des prescriptions générales et permanentes dans les matières traitées par celui-ci.
Ces notes de service seront annexées au Règlement Intérieur.

Il est précisé que toute clause du Règlement qui deviendrait contraire aux dispositions légales, règlementaires ou conventionnelles applicables à la CEPAL du fait de l'évolution de ces dernières, serait nulle de plein droit.

1.3. Publicité

Le présent Règlement Intérieur et ses annexes seront affichés dans les locaux de la CEPAL aux emplacements prévus à cet effet et seront consultables sur le Portail Intranet de l'entreprise.

DISPOSITIONS RELATIVES A L'ORGANISATION DU TRAVAIL ET A LA DISCIPLINE

Article 2 : Organisation du travail et temps de travail

2.1. Horaire de travail

Chaque salarié doit respecter l'horaire de travail en vigueur au sein de l'unité à laquelle il appartient, ainsi que les dispositions légales et conventionnelles relatives au temps de travail.

2.2. Respect de l'horaire de travail

Le personnel en horaire collectif doit respecter l'horaire de travail affiché dans les locaux de travail et se trouver à son poste entre l'heure fixée pour le début du travail et celle prévue pour la fin de celui-ci.
Le personnel qui bénéficie d'horaires variables devra respecter les plages horaires définies par les textes en vigueur dans l'entreprise sachant que le système d'horaire variable doit notamment permettre d'optimiser le fonctionnement des unités et d'améliorer la qualité des services vis-à-vis du réseau commercial.

Il est rappelé que tous les salariés sont soumis aux durées maximales quotidiennes et hebdomadaires et disposent des droits à repos légaux et conventionnels.

Le non-respect des horaires de travail par le salarié peut entraîner l'application de l'une des sanctions prévues par l'article 9 du présent Règlement.

2.3. Temps de travail

Il est interdit d'effectuer un travail personnel sur le lieu de travail.

Les appels téléphoniques extérieurs du personnel sont réservés aux cas exceptionnels et doivent demeurer raisonnables. Il en est de même de l'usage du téléphone portable personnel sur le lieu de travail de façon à ne pas perturber le travail du salarié et/ou de ses collègues de travail.

Le non-respect de ces règles peut entraîner l'application de l'une des sanctions prévues par l'article 9 du présent Règlement.

Article 3 : Accès à l'entreprise

3.1. Conditions d'accès aux locaux

Le personnel n'a accès aux locaux de l'Entreprise que pour l'exécution du contrat de travail. Il n'a aucun droit d'entrer ou de se maintenir sur les lieux de travail pour une autre cause, sauf s'il peut se prévaloir :
- soit d'une disposition légale relative aux droits de la représentation du personnel ;
- soit d'une autorisation délivrée par un responsable ayant le niveau hiérarchique de Directeur.

3.2. Badge d'accès

Les salariés et éventuellement les personnes qui exécutent un travail dans les locaux de l'entreprise se voient attribuer un badge dont la présentation leur permet d'accéder à leur lieu de travail. Ce badge est d'usage strictement personnel et devra être restitué en cas de départ de l'entreprise.

3.3. Personnes extérieures

Il est interdit d'introduire ou de faire introduire dans l'Entreprise des personnes étrangères à celle-ci, sans raison de service, sous réserve des droits des représentants du personnel.

Article 4 : Retards et absences

4.1. Retard

Tout retard et absence doivent être justifiés auprès du responsable hiérarchique. Les retards réitérés non justifiés peuvent entraîner l'une des sanctions prévues par l'article 9 du présent Règlement.

4.2. Absence maladie ou accident

L'absence pour maladie ou accident devra, sauf cas de force majeure, être signalée par tout moyen au plus tôt auprès du responsable hiérarchique et être justifiée dans les 48 heures par l'envoi d'un certificat médical indiquant la durée probable de l'absence.
La production de cette justification est obligatoire, quelle que soit la durée de l'indisponibilité et même si cette dernière est inférieure à 48 heures.

Les prolongations successives d'arrêt de travail pour maladie ou accident doivent être également signalées au responsable hiérarchique, le plus tôt possible et au plus tard le jour prévu initialement pour la reprise. Le certificat médical de prolongation doit être adressé au service de Gestion du Personnel dans les 48 heures.

4.3. Autres absences

Toute absence au travail doit, sauf cas fortuit ou cas de force majeure, faire l'objet d'une autorisation préalable du responsable hiérarchique et être justifiée dans les meilleurs délais et dans la mesure du possible avant la prise de poste.

4.4. Absences injustifiées

Toute absence non justifiée dans ces conditions peut faire l'objet d'une sanction. Il en est de même de toute sortie anticipée sans motif légitime ou sans autorisation, sauf pour les représentants du personnel appelés à s'absenter en raison de leur mandat.

Article 5 : Sorties pendant les heures de travail

5.1. Conditions de sorties

Pour des raisons de sécurité et d'organisation, le salarié ne doit pas quitter son poste de travail sans autorisation de sa hiérarchie, sous réserve des dispositions légales ou conventionnelles. Il

est recommandé, dans la mesure du possible, de formaliser (par écrit ou courriel) une demande d'autorisation.

En ce qui concerne les représentants du personnel, ils devront également, dans la mesure du possible et dans un délai raisonnable, informer leur Hiérarchie préalablement à l'utilisation du crédit d'heures lié à leur mandat.

Article 6 : Usage du matériel de l'Entreprise

6.1. Conditions d'utilisation

Le personnel est tenu de conserver en bon état tout matériel qui lui est confié en vue de l'exécution de son travail ou, pour les représentants du personnel, de l'exécution de leurs fonctions ou du mandat dont ils sont titulaires. Le personnel ne doit pas utiliser ce matériel à d'autres fins, et notamment à des fins personnelles, sans autorisation.
Il est interdit d'envoyer (ou de recevoir) des correspondances personnelles aux frais de l'Entreprise, sauf accord exprès hiérarchique.

Le personnel est tenu de signaler toute défaillance technique ou tout incident à son supérieur hiérarchique.

6.2. Restitution du matériel

Lors de la cessation de son contrat de travail, tout salarié doit, avant de quitter l'entreprise, restituer les matériels (machines, instruments, clés, cartes, badges …) et les documents en sa possession appartenant à l'entreprise.

6.3. Disparition du matériel

Il est interdit d'emporter des objets appartenant à l'entreprise sans autorisation.

En cas de disparition renouvelée et rapprochée d'objets ou de matériel appartenant à l'Entreprise, la Direction peut procéder à une vérification, avec le consentement préalable des intéressés et en leur présence, du contenu des divers effets et objets personnels. Le consentement des salariés devra, dans la mesure du possible, être recueilli en présence de tiers, autres salariés ou représentants du personnel qui pourront également assister à cette opération.
En cas de refus d'un salarié de se prêter à cette vérification, il sera fait appel à un officier de police judiciaire habilité.
La vérification doit s'effectuer dans des conditions qui préservent la dignité et l'intimité des salariés.

Article 7 : Locaux de l'Entreprise

7.1. Usage des locaux de l'entreprise

Les locaux de l'Entreprise sont réservés exclusivement aux activités professionnelles de ses membres ; il ne doit pas y être fait de travail personnel.

Il est interdit :

– d'introduire, dans les lieux de travail, des objets et des marchandises destinées à être vendus, sous réserve des opérations prévues par le législateur dans le cadre des activités sociales et culturelles du Comité d'Entreprise ou d'une centrale d'achats dûment autorisée par la Direction ;

– de faire circuler, sans autorisation de la Direction, des listes de souscription ou de collectes ; seules la collecte des cotisations syndicales et la diffusion des publications et tracts syndicaux peuvent être faites sans autorisation, dans les conditions prévues par la loi ou les accords collectifs applicables à l'Entreprise.

7.2. Affichage dans les locaux

L'affichage est interdit en dehors des emplacements réservés à cet effet ; les affichages régulièrement apposés ne doivent pas être volontairement dégradés ou détruits.

7.3. Parking

Les emplacements de parkings mis à la libre disposition des salariés sont les emplacements non réservés à un usage particulier (*stationnement des véhicules de service par exemple*) ou un utilisateur particulier et matérialisés comme tels. Ces emplacements ne doivent pas être considérés comme un droit et entraîner une occupation permanente de l'emplacement.
Les salariés utilisant ces emplacements sont invités à prendre leurs dispositions en matière d'assurance contre les dommages pouvant être causés à leur véhicule (incendie, vol, actes de vandalisme…), la CEPAL déclinant toute responsabilité en la matière.

Les salariés sont également tenus de respecter les emplacements de stationnement réservés aux personnes handicapées et matérialisés comme tels.

Article 8 : Interdiction et sanctions du harcèlement

8.1. Harcèlement sexuel

Selon les dispositions des articles L 1153-1 et suivants du Code du travail, 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.

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, de formation, de reclassement, d'affectation, de qualification, de classification, de promotion professionnelle, de mutation ou de renouvellement de contrat pour avoir subi ou refusé de subir des faits de harcèlement sexuel tels que définis à l'article L 1153-1, y compris dans le cas mentionné au 1° du même article, si les propos ou comportements n'ont pas été répétés.

Aucun salarié, aucune personne en formation ou en stage, ne peut être sanctionné, licencié ou faire l'objet d'une mesure discriminatoire pour avoir témoigné de faits définis à l'alinéa précédent ou pour les avoir relatés.

Toute disposition ou tout acte contraire est nul.

L'employeur prend toutes dispositions nécessaires en vue de prévenir les faits de harcèlement sexuel. Le texte de l'article 222-33 du Code Pénal est affiché dans les locaux de travail ainsi que dans les locaux ou à la porte des locaux où se fait l'embauche.

Est passible d'une sanction disciplinaire tout salarié ayant procédé aux faits précédemment définis.

8.2. Harcèlement moral

Selon les dispositions des articles L 1152-1 et suivants du Code du travail, aucun salarié ne doit subir les agissements 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.

Aucun salarié, aucune personne en formation ou en stage, ne peut être sanctionné, licencié ou faire l'objet d'une mesure discriminatoire, directe ou indirecte, notamment en matière de rémunération, de formation, de reclassement, d'affectation, de qualification, de classification, de promotion professionnelle, de mutation ou de renouvellement de contrat pour avoir subi ou refusé de subir les agissements définis à l'alinéa précédent ou pour avoir témoigné de tels agissements ou les avoir relatés.

Toute rupture du contrat de travail qui en résulterait, toute disposition ou tout acte contraire est nul.

L'employeur prend toutes les dispositions nécessaires en vue de prévenir les agissements de harcèlement moral. Le texte 222-33-2 du Code Pénal est affiché dans les lieux de travail.

Est passible d'une sanction disciplinaire tout salarié ayant procédé aux agissements précédemment définis.

Une procédure de médiation peut être mise en œuvre par toute personne de l'entreprise s'estimant victime de harcèlement moral ou par la personne mise en cause. Le choix du médiateur fait l'objet d'un accord entre les parties. Le médiateur s'informe de l'état des relations entre les parties. Il tente de les concilier et leur soumet des propositions qu'il consigne par écrit en vue de mettre fin au harcèlement. Lorsque la conciliation échoue, le médiateur informe les parties des éventuelles sanctions encourues et des garanties procédurales prévues en faveur de la victime.

8.3. Autres dispositions relatives au harcèlement

Lorsqu'il survient un litige relatif à des agissements de harcèlement sexuel ou moral, le candidat à l'emploi, à un stage ou à un période de formation en entreprise ou le salarié établit des faits qui permettent de présumer l'existence d'un harcèlement. Au vu de ces éléments, il incombe à la partie défenderesse de prouver que ces agissements ne sont pas constitutifs d'un tel harcèlement et que sa décision est justifiée par des éléments objectifs étrangers à tout harcèlement. Le juge forme sa conviction après avoir ordonné, en cas de besoin, toutes les mesures d'instruction qu'il estime utiles.

Les organisations syndicales représentatives dans l'entreprise peuvent exercer en justice toutes les actions résultant des articles L 1152-1 à L 1152-3 et L 1153-1 à L 1153-4 du Code du travail. Elles peuvent exercer ces actions en faveur d'un salarié de l'entreprise dans les conditions

prévues à l'article L 1154-1, sous réserve de justifier d'un accord écrit de l'intéressé. L'intéressé peut toujours intervenir à l'instance engagée par le syndicat et y mettre fin à tout moment.

Le fait de porter ou de tenter de porter atteinte à l'exercice régulier des fonctions de médiateur est puni d'un emprisonnement d'un an et d'une amende de 3 750 €.

Sont également punis d'un an d'emprisonnement et d'une amende de 3 750 € les faits de discrimination commis à la suite d'un harcèlement moral ou sexuel.

La juridiction peut également ordonner, à titre de peine complémentaire, l'affichage du jugement aux frais de la personne condamnée et son insertion, intégrale ou par extraits, dans les journaux qu'elle désigne.

Article 9 : Sanctions disciplinaires et droits de la défense

9.1. Echelle des sanctions

Le recours aux sanctions s'inscrit dans le cadre des dispositions conventionnelles de la branche Caisse d'Epargne et des dispositions légales et réglementaires, en vigueur, annexées au présent règlement **(ANNEXE 1)**.

Tout agissement considéré comme fautif par l'employeur pourra, en fonction de sa gravité, faire l'objet d'une des sanctions classées ci-après par ordre d'importance.
Les manquements à la discipline et d'une manière générale les fautes professionnelles commises par un agent sont passibles de sanctions disciplinaires.
L'échelle des sanctions est :

- avertissement
- blâme avec inscription au dossier
- mise à pied de 1 à 5 jours
- rétrogradation
- licenciement pour faute

Dans cette échelle, la rétrogradation est l'affectation à un emploi de niveau de classification inférieur liée à une faute disciplinaire dûment constatée.
A compter de la décision définitive de l'employeur et sous réserve de son acceptation par le salarié, celui-ci perçoit la rémunération correspondant à la classification de son nouvel emploi. Les effets salariaux de la rétrogradation ne peuvent être maintenus au-delà d'une durée de 4 ans.

A l'expiration d'un délai de 2 ans, si le salarié n'a pas été entre temps l'objet d'une nouvelle mesure disciplinaire, le blâme avec inscription au dossier est considéré comme non avenu, et les pièces qui y sont relatives sont retirées du dossier.

S'il est reproché à un salarié des faits graves ou en cas d'extrême urgence, l'employeur peut exceptionnellement prononcer la suspension provisoire du salarié en cause. Pendant la durée de sa suspension, le salarié a droit à la moitié au moins de son traitement. Si la peine infligée ultérieurement, après avis du Conseil de Discipline National, n'est pas le licenciement pour faute, le salarié a droit à la totalité de son traitement pour la durée de sa suspension.

9.2. Droit de la défense

Toute sanction, autre que l'avertissement, ne pourra être décidée ou appliquée tant que l'intéressé n'aura pas été dûment convoqué lors d'un entretien au cours duquel l'employeur exposera les griefs portés à son encontre.
Le salarié pourra se faire assister par une personne de son choix appartenant au personnel de l'Entreprise.

Les sanctions de blâme avec inscription au dossier, mise à pied disciplinaire, rétrogradation et licenciement pour faute seront notifiées par un écrit motivé ne pouvant intervenir moins de deux jours ouvrables, ni plus d'un mois après le jour fixé pour l'entretien, sauf dans le cas de saisine du Conseil de Discipline National (CDN).
Dans ce cas, la notification de la sanction au salarié devra intervenir dans le délai d'un mois à compter de l'avis rendu par le CDN.

9.3 La composition, le fonctionnement, les motifs de saisine et la procédure devant le Conseil de Discipline National sont détaillés en ANNEXE 1 du Règlement Intérieur.

DISPOSITIONS RELATIVES A L'HYGIENE ET A LA SECURITE

Article 10 : Hygiène

10.1. Dispositions générales

Il est interdit de pénétrer ou de demeurer dans les locaux de l'entreprise en état d'ivresse ou sous l'emprise de substances stupéfiantes.
Il est également interdit d'introduire, de distribuer, vendre ou consommer, des substances stupéfiantes dans les locaux et dépendances de l'entreprise.
La consommation de boissons alcoolisées dans les locaux de travail est interdite sauf dans des circonstances exceptionnelles, en quantité raisonnable, et avec l'accord de la hiérarchie.
La vente et la distribution de boissons alcoolisées n'est autorisée que dans le cadre des activités sociales et culturelles du Comité d'Entreprise.

Le personnel est tenu d'avoir une présentation correcte et soignée en adéquation avec le poste occupé. De même, dans le respect des droits des personnes et des libertés individuelles, il est rappelé que le personnel est tenu de conserver, au sein de l'entreprise et notamment vis-à-vis de la clientèle et des intervenants extérieurs, une discrétion dans l'expression de ses appartenances politiques, syndicales ou de ses croyances religieuses, et ce, quelle qu'en soit la forme.

Le refus du salarié de se soumettre aux obligations relatives à l'hygiène et à la santé peut entraîner l'une des sanctions prévues par l'article 9 du présent Règlement.

10.2. Interdiction de fumer

Il est strictement interdit de fumer et d'utiliser tout dispositif électromécanique ou électronique générant un aérosol destiné à être inhalé (cigarette électronique) dans tous les locaux et lieux clos et couverts de l'entreprise, à l'exception des espaces mis à la disposition des fumeurs et signalés en tant que tels.

10.3. Visites médicales

En application des dispositions légales en vigueur, le personnel est tenu de se soumettre aux obligations relatives à la médecine du travail : examen d'embauche, examens périodiques, examens de pré-reprise et reprise du travail, examens complémentaires...

Article 11 : Sécurité des personnes et des biens

11.1. Principes généraux

Les dispositions visant à l'application des prescriptions légales et réglementaires relatives à la sécurité figurent dans le présent article et le recueil de sécurité.
Chaque salarié doit se conformer aux instructions relatives à la sécurité du travail (recueil de sécurité, procédures, consignes, formations à la sécurité) données par la Direction ou ses représentants.
Conformément aux instructions de sécurité, chaque salarié doit prendre soin, en fonction de sa formation, et selon ses possibilités, de sa sécurité et de celle de ses collègues de travail.

Il est rappelé que les infractions aux obligations relatives à la Sécurité donneront éventuellement lieu à l'application de l'une des sanctions prévues par l'article 9 du présent Règlement.

11.2. Matériel de secours et dispositif de sécurité

Il est interdit de manipuler les matériels de secours (extincteurs…) en dehors de leur utilisation normale et d'en rendre l'accès difficile.
Il est interdit d'endommager, de détruire tout dispositif de sécurité. Les neutralisations éventuelles seront effectuées dans le cadre de consignes spécifiques délivrées par le Département Protection de la Direction Logistique.

11.3. Incendie

Chaque membre du Personnel doit prendre connaissance du plan d'évacuation des locaux ainsi que des consignes affichées dans chaque lieu de travail aux endroits dédiés.
Chaque membre du personnel doit avoir pris connaissance de ces consignes, et devra les appliquer y compris à l'occasion d'exercices de simulation ; en outre, il doit avoir conscience de la gravité des conséquences possibles de leur non-respect. En cas d'incendie ou menace d'incendie, tout membre du personnel est tenu d'appliquer les consignes affichées sur les panneaux prévus à cet effet.

11.4. Installations électriques, appareils électriques

Seules les personnes possédant un titre d'habilitation règlementaire valide peuvent intervenir sur les installations électriques (prises de courant, luminaires, fusibles…) ou pour des travaux de nature électrique au sein de la CEPAL.

Seuls les appareils électriques mis à la disposition par la CEPAL peuvent être utilisés dans les locaux et conformément à leur destination. En raison du risque d'électrocution que peuvent présenter certaines manipulations d'appareils électriques, il est interdit au personnel non habilité de procéder à des démontages pour vérification ou réparation de ce type d'appareils. En cas de panne ou de défectuosité, le personnel utilisateur doit, après en avoir référé à sa hiérarchie, faire appel à la Direction Logistique, qui décidera des moyens à mettre en œuvre.

11.5. Accident au cours du travail

Tout accident, même léger, survenu au cours du travail (ou du trajet), doit être porté à la connaissance de la hiérarchie et du service de Gestion du Personnel, le plus rapidement possible, dans la journée même de l'accident ou au plus tard dans les 24 heures, sauf cas de force majeure, impossibilité absolue ou motif légitime.

11.6. Usage des véhicules de service

L'usage des véhicules de service est réservé exclusivement à des fins professionnelles, excluant ainsi tout déplacement d'ordre privé.

Tout salarié, dont les attributions comportent l'utilisation d'un véhicule de l'entreprise, doit respecter les obligations suivantes :

- avoir le permis de conduire valide adapté au véhicule ;
- posséder les documents administratifs du véhicule qu'il devra restituer, ainsi que les clés du véhicule, dès la fin de la mission ;
- respecter les consignes du Code de la route ;

- signaler immédiatement à la Direction Logistique les défectuosités, anomalies et incidents (vol, accident…) nés pendant l'utilisation du véhicule et en faire une confirmation par écrit ;
- ne pas conduire en état d'ivresse ou sous l'emprise de stupéfiants ;
- ne pas confier le véhicule à une tierce personne ;
- veiller à ce que le véhicule soit fermé à clé et, dans la mesure du possible, qu'aucun titre de circulation, matériel ou document confidentiel ne soient laissé à bord pendant et en dehors des périodes d'utilisation.

Les infractions au Code de la route commises par un salarié à l'occasion de l'utilisation d'un véhicule mis à sa disposition par l'entreprise relèvent de sa responsabilité pénale et pécuniaire. Aussi, il devra impérativement communiquer à l'employeur son identité et ses coordonnées dans les délais impartis et s'acquittera personnellement du montant des amendes qui pourraient en découler.

11.7. Droit de retrait

En application de l'article L 4131-1 du Code du travail, le salarié peut se retirer de toute situation de travail dont il a un motif raisonnable de penser qu'elle présente un danger grave et imminent pour sa vie ou sa santé. Dans ce cas, il doit alerter immédiatement son supérieur hiérarchique ainsi que le Département Protection de la Direction Logistique.

Les représentants du personnel au CHSCT seront informés de cette situation le plus rapidement possible.

11.8. Transmission et enregistrement d'image de vidéosurveillance

La loi du 21 janvier 1995 d'orientation et de programmation relative à la sécurité autorise la transmission et l'enregistrement d'images prises dans des lieux et établissements ouverts au public particulièrement exposés à des risques d'agression ou de vol, par le moyen de vidéosurveillance, afin d'y assurer la sécurité des personnes et des biens.

Dans ce but, le champ de prise de vues des systèmes de vidéosurveillance est une entrée ou sortie de bâtiment, un lieu de passage ou de circulation, un espace sensible, ou un libre-service bancaire en fonction du type de prévention traitée. Il doit permettre au télésurveilleur, et si besoin au Département Protection, d'effectuer une levée en cas de doute, d'alarme ou d'appel à l'aide.

Le système d'enregistrement vidéo est destiné essentiellement à aider la Police dans l'identification d'éventuels intrus, vandales ou malfaiteurs.
Les enregistrements sont conservés un minimum de 7 jours et un maximum de 30 jours hormis dans les cas d'enquête de flagrant délit, enquête préliminaire ou d'information judiciaire.

Le droit d'accès d'un salarié aux images le concernant sera exercé par écrit, auprès du Responsable de la Protection.

11.9. Enregistrement des communications téléphoniques des salariés participant à la relation commerciale

La CEPAL organise dans des conditions conformes aux lois et règlements en vigueur et après information du Comité d'Entreprise, l'enregistrement des conversations téléphoniques des négociateurs d'instruments financiers et des salariés qui, sans être négociateurs, participent à la relation commerciale avec des donneurs d'ordres ou opèrent des transactions commerciales.
Tous les enregistrements téléphoniques sont conservés sur un support fidèle et durable.

Le salarié dont les conversations téléphoniques sont susceptibles d'être enregistrées en sera informé au préalable par écrit et pourra obtenir l'audition d'un enregistrement en en faisant la demande écrite auprès du Responsable de la Conformité. Dans les mêmes conditions, les salariés seront informés de la conservation desdits enregistrements.

11.10. Utilisation d'outils techniques d'enregistrements vidéo et sonores

La CEPAL peut être amenée à utiliser des techniques d'enregistrements vidéo et sonores en vue d'atteindre une certaine qualité de service lors de réunions professionnelles, notamment celles du Conseil d'Orientation et de Surveillance, de web-conférences, visioconférences, audioconférences…

Les personnes susceptibles d'être enregistrées en seront avisées au préalable et pourront obtenir l'audition d'un enregistrement en en faisant la demande écrite auprès du Responsable de la Conformité.

CONFORMITE ET DEONTOLOGIE

12.1. Obligation générale de conformité et de déontologie

De manière générale, dans l'exécution des tâches qui lui sont confiées, chaque membre du personnel est tenu de respecter les instructions qui lui sont données par ses supérieurs hiérarchiques et se doit d'agir d'une manière honnête, loyale et professionnelle afin de garantir l'intégrité de la profession.

Il est à ce titre tenu de respecter les règles et procédures établies par le service de la Conformité ainsi que les règles internes, procédures et instructions de sa Hiérarchie, mises en place afin d'assurer le respect des règles déontologiques et préserver l'objectivité et l'impartialité du conseil à la clientèle.

Ces règles prévoient notamment le respect :
- de la confidentialité, du secret professionnel et de la prévention de la circulation indue des informations privilégiées
- du traitement des conflits d'intérêts
- de la lutte contre le blanchiment, le financement du terrorisme
- de la lutte contre la fraude interne.

Il est rappelé que le non-respect des règles de conformité et de déontologie annexées au présent Règlement Intérieur **(ANNEXE 2)** constitue une faute et est susceptible d'entraîner, selon les circonstances, l'application de l'une des sanctions prévues par l'article 9 du Règlement Intérieur.

Leur non-respect est par ailleurs susceptible, selon les cas, de constituer un délit pénal.

Les dispositions contenues dans l'annexe 2 ont vocation à être modifiées en fonction des évolutions législatives, règlementaires ou conventionnelles.

12.2. Contrôle du respect des obligations de Conformité et de Déontologie

La surveillance des opérations effectuées sur les comptes des salariés et le contrôle du respect des obligations auxquelles ils sont astreints sont confiés par l'employeur aux Directions en charge de l'Audit et de la Conformité.

Les salariés sont informés que les données les concernant, traitées dans le cadre du dispositif de lutte contre la fraude interne et les manquements déontologiques, sont destinées aux personnes habilitées de la CEPAL. Les salariés disposent d'un droit d'accès aux informations nominatives les concernant ainsi que d'un droit de rectification dans les conditions de la Loi Informatique, Fichiers et Libertés du 6 janvier 1978, auprès du Directeur de la Conformité.

Le traitement et la conservation des données du dispositif de lutte contre la fraude interne et les manquements déontologiques sont effectués conformément aux déclarations faites à la CNIL.

DISPOSITIONS RELATIVES A L'UTILISATION DES MOYENS INFORMATIQUES ET DE COMMUNICATION ELECTRONIQUE

13.1. Obligation générale

L'ensemble des moyens informatiques et de communication électronique doit être utilisé conformément aux dispositions prévues par la **Charte d'utilisation des moyens informatiques et de communication électronique annexée au présent Règlement Intérieur (ANNEXE 3)**.

ENTREE EN VIGUEUR ET MODIFICATIONS DU REGLEMENT INTERIEUR

Article 14 : Date d'entrée en vigueur

14.1. Entrée en vigueur

Ce règlement entrera en vigueur le
Il a été préalablement affiché conformément aux dispositions du Code du travail et déposé au greffe du Conseil de Prud'hommes de Clermont-Ferrand.

14.2. Procédure de consultation

Conformément à l'article L 1321-4 du Code du travail, ce Règlement a été soumis aux membres du Comité d'Entreprise, ainsi que pour les matières relevant de sa compétence, au Comité d'Hygiène, de Sécurité et des Conditions de Travail.
Les avis émis par ces instances ont été adressés à l'Inspecteur du Travail en même temps que deux exemplaires du Règlement.

14.3. Procédure de modification

Toute modification ultérieure ou tout retrait de clause de ce règlement serait, conformément au Code du travail, soumis à la même procédure, étant entendu que toute clause du Règlement qui deviendrait contraire aux dispositions légales, règlementaires ou conventionnelles applicables à la CEPAL du fait de l'évolution de ces dernières, serait nulle de plein droit.

Fait à Clermont-Ferrand, le

Paul KERANGUEVEN
Président du Directoire

CAISSE D'EPARGNE
D'AUVERGNE ET DU LIMOUSIN

Annexe 1 : COMPOSITION, FONCTIONNEMENT, MOTIFS DE SAISINE ET PROCEDURE DEVANT LE CONSEIL DE DISCIPLINE NATIONAL (CDN)

EXTRAIT DE L'ACCORD SUR LE CONSEIL DE DISCIPLINE NATIONAL DU 12 JUILLET 2013

PARTIE 1 : LA SAISIE DU CDN

➢ Article 1 : Les cas de saisine

Le salarié a la possibilité de saisir le CDN en cas de projet de rétrogradation ou de projet de licenciement pour motif disciplinaire envisagé à son encontre par son employeur. Le projet de licenciement pour faute lourde n'est pas visé par le présent accord.

Le CDN est alors chargé de formuler un avis.

➢ Article 2 : modalités de saisine

Dans les 5 jours ouvrables qui suivent l'entretien préalable (que le salarié se soit présenté ou non), l'employeur informe le salarié par lettre recommandée avec accusé de réception (LRAR), de sa volonté de poursuivre une procédure de licenciement pour motif disciplinaire (hors faute lourde) ou de rétrogradation et indique expressément la possibilité pour le salarié de saisir le CDN, le délai saisine et les modalités de celle-ci. Il lui rappelle également qu'à défaut de saisine dans le délai imparti et dans le respect des modalités de celle-ci ou si le salarié indique expressément ne pas vouloir saisir le CDN, il pourra poursuivre la procédure de licenciement ou de rétrogradation engagée.

La saisine du CDN intervient sous la forme d'une LRAR envoyée par le salarié au secrétariat du CDN, avec copie à l'employeur.

Le salarié dispose d'un délai de **5** jours ouvrables, à compter de la première présentation du courrier de l'employeur, lui confirmant le projet de licenciement pour motif disciplinaire ou rétrogradation, pour saisir le CDN.
La saisine est accompagnée du courrier de l'employeur.

PARTIE 2 : LE FONCTIONNEMENT DU CDN

➢ Article 3 : Convocation devant le CDN

Le secrétariat, assuré par l'organe central, examine la conformité de la saisine et fixe la date de réunion. Il convoque les parties par LRAR ou par courriel dès lors que ce dernier permet l'obtention d'un accusé de réception.

➢ Article 4 : Procédure devant le CDN

L'employeur envoie ses éléments écrits au CDN, copie salarié, dans un délai de **8** jours calendaires à compter de la première présentation du courrier de saisine du salarié ; cet envoi intervient sous la forme d'une LRAR au salarié et peut être réalisé par courrier ou par courriel au secrétariat du CDN dès lors que ce dernier permet l'obtention d'un accusé de réception.

A compter de la date de réception de la saisine du CDN par le secrétariat de l'organe central, le salarié dispose de 15 jours calendaires pour transmettre ses éventuels éléments écrits au CDN, copie employeur ; ces envois sont réalisés par LRAR.

Toute procédure judiciaire, concernant le même dossier, engagée par le salarié avant que le CDN ait rendu un avis, met fin à la procédure de recours.

Le secrétariat envoie les dossiers à l'ensemble des membres du CDN convoqués, au minimum 6 jours calendaires avant la réunion. Cet envoi peut être réalisé par courrier ou par courriel dès lors que ce dernier permet l'obtention d'un, accusé de réception.

- **Article 5 : Réunion du CDN**

L'absence du demandeur à la réunion ne fait pas obstacle à la tenue de la réunion.

Le salarié peut être assisté d'une personne de son choix appartenant au personnel de l'entreprise ou d'une entreprise de la branche.

L'employeur est représenté par une personne de son choix appartenant au personnel de l'entreprise.

La parité est respectée dès lors que chaque délégation est représentée par au moins deux membres.

- **Article 6 : Avis du CDN**

A l'issue de la réunion, le CDN rend soit un avis commun, soit un avis par délégation.

Chaque délégation élabore son avis à huis clos.

Cet avis doit être formulé hors de la présence du salarié.

Une fois cet avis retranscrit par le secrétariat du CDN, il est communiqué par LRAR au salarié et par courriel à l'employeur, lequel notifie sa décision au salarié.

En cas de notification d'une rétrogradation par l'employeur et de refus de la rétrogradation par le salarié, le CDN ne peut être saisi dans le cadre d'un projet de licenciement pour motif disciplinaire portant sur l'examen des mêmes faits.

PARTIE 3 : LA COMPOSITION DU CDN

- **Article 7 : Composition du CDN**

Le CDN est composé de deux délégations, constituées comme suit :

I- Les parties constatent que les mandats en cours des membres titulaires et suppléants courent jusqu'au 23 juin 2014.
En conséquence, et jusqu'à cette date la composition du CDN est inchangée.

II- A compter du 24 juin 2014, la nouvelle composition du CDN est la suivante :

1- Membres représentant les salariés

Neuf membres représentent les salariés.

Après attribution d'un siège à chaque organisation syndicale représentative, les sièges restant sont répartis entre les organisations syndicales sur la base des résultats en nombre de voix recueillies au 1er tour des élections des titulaires des comités d'entreprise ou d'établissement ou délégation unique du personnel, ou à défaut délégués du personnel des entreprises de la branche, en application de la règle de la plus forte moyenne.

Pour l'appréciation de cette répartition, il est procédé à l'analyse des résultats des élections constatés lors de la mesure d'audience des organisations syndicales dans la branche.

Pour le premier cycle d'application de ce texte, le nombre de sièges est calculé à la date d'entrée en vigueur des présentes dispositions et ce, pour la durée restant à courir jusqu'à la prochaine mesure d'audience des organisations syndicales dans la branche.

Cette désignation se fait parmi les salariés des entreprises de la branche.

Les mandats de ces membres prennent fin de façon anticipée par la démission du mandat de membre du CDN ou de façon automatique, par la perte de la qualité de salarié d'une entreprise de la branche.

Tout remplacement définitif d'un membre nécessite une nouvelle désignation par l'organisation syndicale qui avait procédé à la première désignation, pour la durée du mandat restant à courir.

2- Membres représentant les employeurs

L'organe central établit annuellement une liste de membres représentant les employeurs.

Cette liste est communiquée aux organisations syndicales ayant des membres représentant les salariés au CDN.

- **Article 8 : Composition des délégations à chaque réunion**

Trois membres issus de la liste employeur sont désignés par l'organe central pour chaque réunion.

La délégation salariale est composée de trois membres.

La parité est respectée dès lors que la réunion se tient en présence de deux membres minimum par délégation.

Aucune des deux délégations ne peut comprendre de membres appartenant à l'entreprise dont relève le salarié qui a saisi l'instance.

Pour chaque réunion de CDN le secrétariat appelle les membres de la délégation salariale par ordre alphabétique, jusqu'à ce que la délégation soit complète ; pour la réunion suivante, l'appel par ordre alphabétique se fait à compter du nom du dernier membre retenu à la réunion précédente.

La présidence du CDN revient alternativement à chaque délégation. Les années paires, elle est assurée par un représentant des employeurs. Les années impaires par un représentant du personnel.

Le secrétaire du CDN assiste aux réunions.

Chaque participant est tenu à une obligation de discrétion à l'égard des éléments confidentiels nécessaires à l'examen du dossier.

CAISSE D'EPARGNE
D'AUVERGNE ET DU LIMOUSIN

Annexe 2 : CHARTE DE CONFORMITE ET DE DEONTOLOGIE

Article 1 : Confidentialité et secret professionnel

1.1. Confidentialité

Une information confidentielle inclut toute information non publique qui pourrait être utilisée par les concurrents et/ou être dommageable à la CEPAL, au Groupe ou à ses clients si celle-ci était diffusée.
Elle inclut notamment les informations confidentielles relevant de la propriété intellectuelle de l'entreprise, de l'activité de l'entreprise, des plans marketing et commerciaux, des bases de données, des dossiers, des projets économiques, des informations sur les rémunérations, des données financières et rapports non publiés, des informations confiées par les partenaires, fournisseurs et clients…

Afin de garantir la protection des informations confidentielles, les salariés de la CEPAL doivent respecter les consignes suivantes :

- les documents contenant des informations confidentielles non publiques devront être conservés en lieu sûr ;
- les conversations professionnelles sensibles dans le cadre du travail, en personne ou par téléphone, devront être évitées dans des endroits publics et une attention toute particulière devra être portée lors de l'utilisation d'ordinateurs portables et autres équipements dans des endroits publics ;
- les courriels et documents attachés contenant des informations confidentielles non publiques devront être traités avec une vigilance similaire ;
- la réception de visiteurs dans des zones ou locaux où se trouvent stockées des informations confidentielles non publiques devra être encadrée pour éviter toute divulgation dommageable à l'entreprise.

1.2. Secret professionnel

1.2.1. Obligations générales

Par application de l'article L 511-33 du Code monétaire et financier, la CEPAL et ses salariés sont soumis au secret professionnel.

Le non-respect de cette obligation est sanctionné pénalement par l'article 226-13 du Code pénal qui prévoit que la révélation d'une information à caractère secret par une personne qui en est dépositaire, soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15 000€ d'amende.

Le non-respect de cette obligation est sanctionné civilement par la responsabilité civile et le paiement de dommages et intérêts soit à la charge personnelle du salarié soit à la charge de l'établissement, soit des deux.

Ainsi, tout salarié de l'entreprise et toute autre personne y travaillant à quelque titre que ce soit est tenu au respect du secret professionnel et de la confidentialité la plus stricte à l'égard de toute information non publique dont il pourrait avoir connaissance, quelle qu'en soit la source, dès lors qu'elle a été obtenue dans le cadre de l'activité professionnelle.

Notamment, à l'intérieur de l'Etablissement, le personnel est tenu à l'obligation de discrétion à l'égard des personnes n'ayant pas à connaître, du fait de leurs fonctions, des informations confidentielles.

1.2.2. Champ d'application

Le secret professionnel couvre notamment :
- l'identité des clients, leurs opérations et les renseignements qu'ils communiquent ;
- les autres informations confidentielles reçues dans l'exercice des fonctions et des mandats sociaux ou de représentation confiés aux salariés de l'établissement ;
- les offres des fournisseurs, de même que le contenu des contrats signés. Ces informations ne peuvent en aucun cas être diffusées sous quelque forme que ce soit à l'extérieur de la CEPAL sauf approbation expresse de la Hiérarchie.

La divulgation de ces éléments doit être limitée :
- à l'intérieur de l'entreprise, à ceux qui ont à les connaître dans l'exercice de leurs fonctions ;
- à l'extérieur, à des tiers liés eux-mêmes par des clauses de confidentialité, le respect du secret professionnel ou intervenant sur mandat de l'autorité publique.

1.2.3. Dérogations spécifiques

La loi a prévu des dérogations à l'opposabilité du secret bancaire dans un certain nombre de cas notamment :
- à l'égard de l'autorité judiciaire lors des procédures pénales et aux requêtes d'un juge saisi au civil ;
- à l'égard des autorités bancaires et boursières notamment l'Autorité des Marchés Financiers (AMF), l'Autorité de Contrôle Prudentiel et de Résolution (ACPR), la Banque de France ;
- à l'égard de TRACFIN lorsqu'il y a soupçon d'opérations de blanchiment des capitaux ;
- à l'égard de la Commission Départementale chargée du surendettement des personnes physiques ;
- à l'égard de l'administration fiscale.

Toute demande de levée du secret bancaire, qu'elle qu'en soit la forme (écrite ou verbale), doit être transmise au préalable au Responsable du Département Juridique de l'établissement et tout document ou matériel ne peut, en aucune circonstance, être transmis à des autorités judiciaires, bancaires, boursières ou administratives en réponse à une demande d'informations sans l'approbation expresse du Responsable du Département Juridique et/ou du Responsable de la Conformité.

Un salarié qui apprend qu'il fait l'objet d'une enquête réglementaire dans le cadre de ses activités au sein de la CEPAL doit immédiatement en informer le Responsable du Département Juridique et/ou du Responsable de la Conformité.

1.2.4. Responsabilité et implication de la hiérarchie

Les responsables hiérarchiques doivent s'assurer, dans le cadre de leurs attributions, de la connaissance et du respect du secret professionnel au sein des unités dont ils ont la charge. Ils veillent à ce que la confidentialité des opérations des clients comme du groupe soit préservée, notamment en sensibilisant à ce sujet les salariés de leur unité, et en vérifiant l'application des procédures organisées par l'établissement au sein de leurs unités.

Article 2 : Règles relatives à la circulation indue d'informations confidentielles et privilégiées

La CEPAL dispose d'un dispositif interne de contrôle de l'utilisation d'informations matérielles non publiques.
Ce dispositif s'articule autour d'un ensemble de règles établies afin d'empêcher la diffusion d'informations matérielles non publiques, confidentielles et privilégiées, par les salariés de la CEPAL qui seraient amenés à en avoir connaissance dans le cadre de l'exercice de leurs fonctions.

2.1. Information privilégiée

L'usage d'une information privilégiée, c'est-à-dire d'une information non encore divulguée de nature à influer sur le cours d'une valeur est constitutif du délit d'initié ou du délit de divulgation d'information, délits prévus et réprimés par l'article 10-1 modifié de l'ordonnance du 28 septembre 1967.

2.2. Obligation de déclaration

Les salariés doivent strictement veiller à ne pas se trouver en situation d'infraction à cette réglementation. Plus particulièrement, ils s'engagent à respecter les procédures organisées par leur établissement aux fins d'assurer le respect de cette réglementation et notamment de prévenir la circulation indue d'informations privilégiées. Ils veillent à informer le responsable de la Conformité de l'établissement de tout dossier sensible qu'ils sont amenés à traiter.

2.3. Respect des procédures

Les salariés doivent respecter les procédures mises en œuvre pour organiser :
- la séparation des différentes unités de l'établissement susceptibles de générer des conflits d'intérêts. Le but est d'empêcher la diffusion d'informations confidentielles entre métiers, entre départements, entre maison mère et filiales… ;
- les conditions dans lesquelles le Responsable de la Conformité peut autoriser, dans des cas particuliers, la transmission d'informations confidentielles entre unités.

2.4. Obligation d'information

Tout salarié concourant à l'activité de conseil en gestion, d'analyse financière ou d'activités d'ingénierie financière ou de gestion pour compte propre est tenu de respecter les règles de circulation des informations confidentielles et privilégiées.
Informé de l'existence d'une information privilégiée dans une unité de l'établissement, le Responsable de la Conformité décide de l'opportunité et du moment de l'inscription de la valeur sur une liste de surveillance ou d'interdiction.

2.5. Responsabilité et implication de la hiérarchie

Les responsables hiérarchiques doivent s'assurer, dans le cadre de leurs attributions, de la connaissance et du respect des règles de circulation d'informations confidentielles et privilégiées au sein des unités dont ils ont la charge. Ils veillent à ce que la confidentialité des opérations des clients comme de l'établissement soit préservée, notamment en sensibilisant à ce sujet les salariés de leur unité, et en vérifiant l'application des procédures organisées par l'établissement au sein de leurs unités.

Article 3 : Délit d'initié

Les salariés et dirigeants qui disposent, à l'occasion de l'exercice de leur profession ou de leurs fonctions, d'informations privilégiées sur les perspectives ou la situation d'un émetteur dont les titres sont négociés sur un marché réglementé ou sur les perspectives d'évolution d'un instrument financier admis sur un marché réglementé, encourent les sanctions prévues aux articles 465-1 et suivants du Code monétaire et financier s'ils :

- réalisent ou se permettent de réaliser, soit directement, soit par personne interposée, une ou plusieurs opérations avant que le public ait connaissance de ces informations ;
- communiquent à un tiers en dehors du cadre normal de leur profession ou de leurs fonctions ;
- exercent ou tentent d'exercer, directement ou par personne interposée, une manœuvre ayant pour objet d'entraver le fonctionnement régulier d'un marché réglementé en induisant autrui en erreur ;
- répandent dans le public par des voies et moyens quelconques des informations fausses ou trompeuses de nature à agir sur les cours.

Article 4 : Exercice de l'activité professionnelle et conflits d'intérêts

4.1. Conflits d'intérêts

Il y a « conflit d'intérêts » lorsque les intérêts individuels d'une personne entrent, sont susceptibles d'entrer ou semblent entrer en conflit d'une façon ou d'une autre avec les intérêts de la CEPAL.

Le conflit d'intérêts se définit comme une situation dans laquelle le salarié ou le représentant de la CEPAL peut être amené à ne pas agir en toute indépendance et/ou objectivité.

Une situation de conflit d'intérêts peut survenir :

- lorsqu'un salarié engage des actions ou détient des intérêts (commerciaux, financiers ou autres) qui peuvent nuire à la réalisation objective et efficace de son travail pour l'entreprise

- lorsqu'un salarié, ou un membre de sa famille[1], reçoit des avantages personnels indus, ou s'enrichit personnellement ou tire profit d'informations confidentielles

- lorsqu'un salarié, ou un membre de sa famille, détient une participation financière dans une entreprise ayant des relations commerciales importantes avec la CEPAL ou le Groupe ou s'il exerce une activité à l'extérieur de l'établissement qui peut mettre en cause sa loyauté ou son indépendance de jugement.

Aussi, tout salarié doit s'interdire de prêter son concours à une personne morale ou physique, institution ou organisme associés et partenaires, dont l'activité professionnelle présente un caractère concurrentiel par rapport aux activités de la CEPAL ou le plaçant dans une position de conflit d'intérêts avec la société ou ses clients, sauf autorisation expresse du Directoire.

[1] *conjoint, ascendants, descendants, frères et sœurs (collatéraux), belle-famille (beaux-parents, beau-fils, belle-fille) et toute personne partageant le foyer familial.*

Les mesures de prévention et de sensibilisation peuvent être insuffisantes pour éliminer la totalité des situations de conflits potentiels. Dans ce cas, il revient au niveau hiérarchique supérieur des salariés confrontés à ce risque, de gérer en liaison avec le Responsable de la Conformité, la situation. Cette gestion implique en tout état de cause un traitement équitable des clients.

4.2. Opérations des salariés pour leur propre compte

4.2.1. Dispositions générales

4.2.1.1. Opérations pour compte propre ou personnes proches

Un salarié devra toujours privilégier la Banque à Distance (service Direct Ecureuil via Internet « DEI » ou « C Ma Banque ») ou à défaut s'adresser à un autre salarié de son agence de rattachement professionnel ou de domiciliation bancaire pour réaliser des opérations sur ses comptes, ceux de sa famille ou sur les comptes pour lesquels il bénéficie d'une procuration.

De même, tout salarié est tenu de privilégier la Banque à Distance ou à défaut s'adresser à un autre salarié de son agence de rattachement professionnel ou de domiciliation bancaire pour réaliser des opérations de bourse.
Les salariés s'interdisent :

- de passer des opérations de bourse dans la journée sans couverture
- d'émettre ou d'exécuter des ordres sur instruments financiers de manière privilégiée par rapport aux ordres de la clientèle.

4.2.1.2. Concours, tarifications et procurations pour compte propre ou personnes proches

Tout salarié est tenu de ne pas accorder de concours (crédits, découverts, facilités de caisse…), remises commerciales et non-tarification à lui-même, à un membre de sa famille ou à une personne morale dans laquelle lui-même ou un membre de sa famille a des intérêts.

Tout salarié doit s'interdire de recevoir de procuration de tiers.
Toutefois, en matière de procuration, la CEPAL accepte que ses salariés soient mandataires sur les comptes de leur conjoint, concubin(e), partenaire d'un PACS, ascendants, descendants, ou frères et sœurs (collatéraux) ou de personnes morales. Une déclaration préalable auprès de la Direction des Ressources Humaines devra être effectuée pour les procurations données à un salarié par les personnes morales et les membres de la famille du salarié autres que le conjoint, concubin(e), partenaire d'un PACS, ascendants et descendants.

4.2.1.3. Opérations sur comptes propres pour le compte de tiers

Tout salarié est tenu de ne pas utiliser ses comptes personnels pour faire transiter des opérations pour des tiers aux lieux et places des comptes prévus à cet effet.
Tout salarié doit s'interdire de recevoir et conserver des dépôts de tiers (espèces, livrets, clefs de coffre…).

4.3. Postes d'administrateurs et autres activités par participations

Bien que des activités en dehors de la CEPAL ne soient pas nécessairement sources de conflit d'intérêts, un conflit pourrait survenir entre le poste occupé au sein de la CEPAL et les activités exercées.

4.3.1. Postes d'administrateurs et mandats sociaux

Les salariés sont tenus de déclarer au Responsable de la Conformité leurs sièges dans les conseils d'administration, conseils de surveillance, directoire ou autres organes de direction dans les sociétés françaises ou étrangères.

Aucun salarié ne peut exercer simultanément, à un titre principal ou accessoire des fonctions générant des conflits d'intérêt au sens de la réglementation ou des codes de bonne conduite professionnels applicables à la société.

Les salariés sont tenus de déclarer au Responsable de la Conformité les mandats sociaux qu'ils occupent dans des sociétés détenues à titre personnel ainsi que les intérêts familiaux ou de proches susceptibles de provoquer des conflits d'intérêts dans l'exercice de la fonction occupée.

Les salariés s'engagent à déclarer au Responsable de la Conformité tout nouveau mandat social et toute suppression de mandat social existant.

4.3.2. Participations financières ou commerciales

Des conflits d'intérêts peuvent survenir lorsqu'un salarié ou un membre de sa famille détient une participation dans une société ayant des liens commerciaux significatifs, réguliers ou ponctuels avec la CEPAL ou une entité du Groupe.

Avant d'effectuer ce type d'investissement à titre personnel, les salariés devront consulter leur supérieur hiérarchique ou le Responsable de la Conformité afin qu'une autorisation préalable soit obtenue auprès du Directoire de la CEPAL.

Les salariés devront également être vigilants quant aux participations détenues dans des sociétés extérieures et qui pourraient mettre en cause leur loyauté et/ou compromettre leur indépendance de jugement.

Les transactions commerciales qui profitent à des membres de la famille du salarié ou à des proches, telles que l'attribution d'un contrat commercial à une société dans laquelle ils détiennent une participation de contrôle ou un autre type de participation significative, peuvent induire ou faire naître un conflit d'intérêts.
Les salariés devront consulter leur supérieur hiérarchique et/ou le Responsable de la Conformité avant de conclure de telles transactions.

4.3.3. Autres engagements en dehors du Groupe

Chaque salarié a le devoir de s'assurer que toutes ses activités externes, qu'elles soient caritatives ou de bénévolat, ne risquent pas d'entraîner un conflit d'intérêts ou ne sont pas contradictoires avec les activités qu'il exerce au sein du de la CEPAL.

Article 5 : Salariés « sensibles » ou « particulièrement sensibles »

5.1. Les salariés considérés comme « sensibles » ou « particulièrement sensibles »

Certains salariés qui, ont ou peuvent régulièrement avoir accès, en raison de la nature de leur fonction ou de leurs tâches, à une ou des informations privilégiées ou confidentielles ou que leur fonction expose à se trouver en situation de conflit d'intérêts sont considérés comme « sensibles ».

Il s'agit notamment des personnes occupant des fonctions de marché primaire et de montage, les analystes financiers, les vendeurs et les opérateurs de marché et en particulier les détenteurs de cartes professionnelles, leurs assistants, ainsi que leurs supérieurs hiérarchiques.

5.1.1. Obligations générales des salariés « sensibles » ou « particulièrement sensibles »

Ils ont une interdiction d'intervenir pour leur propre compte sur les marchés ou sur des instruments financiers sur lesquels ils sont susceptibles, de par leurs fonctions, d'avoir une information confidentielle ou privilégiée, sauf autorisation expresse du Responsable de la Conformité durant les périodes autorisées.

5.1.2. Le contrôle des opérations des salariés « sensibles » ou « particulièrement sensibles »

Le Responsable de la Conformité est habilité à procéder à toute investigation pour s'assurer du respect de ces dispositions.
Conformément aux dispositions légales, le Responsable de la Conformité et les salariés dédiés à cette mission se portent garants de la confidentialité des informations reçues.

5.2. Les obligations des salariés « sensibles »

Ils sont alors soumis au régime de transparence de leurs opérations sur instruments financiers.
La liste des salariés « sensibles » est tenue et mise à jour par le responsable de la Conformité. Ce dernier avise individuellement et par écrit les salariés de leur appartenance à la catégorie des salariés sensibles.

Les comptes d'instruments financiers visés par ce dispositif sont les comptes d'instruments financiers ouverts au nom du salarié sensible et les comptes d'instruments financiers joints, indivis ou pour lesquels le salarié sensible dispose d'une procuration.

Les salariés « sensibles » s'engagent à déclarer immédiatement au responsable de la Conformité toute nouvelle ouverture ou fermeture de comptes d'instruments financiers.

Les salariés « sensibles » peuvent détenir des comptes d'instruments financiers.
Il s'agit des comptes titres (y compris P.E.A.) sur lesquels sont inscrits des instruments financiers (actions, obligations, warrants, OPCVM…) et qui ne font pas l'objet d'un mandat de gestion. Le salarié peut agir directement sur ses comptes en passant lui-même ses instructions d'achat ou de vente de titres.

Les obligations concernant les comptes titres :
- déclarer au Responsable de la Conformité les comptes d'instruments financiers ;
- domicilier les comptes d'instruments financiers dans un établissement agréé par l'AMF[2] ou une autorité de tutelle européenne.

Les obligations concernant les opérations :
- déclarer, sous 48 h, au Responsable de la Conformité les opérations effectuées sur les instruments financiers. Cette obligation ne s'applique pas aux opérations portant sur des OPCVM ;

[2] *ce qui exclut les établissements exotiques sans mettre en cause le principe prévalant de libre choix par le salarié de l'établissement de domiciliation.*

- respecter les restrictions ponctuelles imposées par le Responsable de la Conformité et portées à la connaissance des personnes sensibles.

Les salariés « sensibles » peuvent détenir des comptes titres sous mandat de gestion. Ils doivent satisfaire les obligations suivantes :
- déclarer au Responsable de la Conformité les comptes titres sous mandat de gestion ;
- communiquer une copie des relevés d'opérations sur simple demande au Responsable de la Conformité.

5.3. Obligations propres à certains salariés « particulièrement sensibles »

Sont considérés comme salariés « particulièrement sensibles », les salariés qui peuvent disposer, suivant l'organisation de leur service et leurs fonctions, d'un nombre important d'informations confidentielles et privilégiées.

Ce dispositif concerne :
- les membres du Directoire, du Comité de Direction Générale, du Comité Exécutif et les personnes qui y assistent régulièrement ;
- les personnes dont les fonctions selon leur nature les rendent particulièrement sensibles, sont désignées par le Membre du Directoire ou du Comité de Direction Générale ou du Comité Exécutif dont elles dépendent qui en avisent le Responsable de la Conformité afin que ce dernier informe les intéressés.

Les comptes d'instruments financiers visés par ce dispositif sont les comptes d'instruments financiers ouverts au nom du salarié « particulièrement sensible » et les comptes d'instruments financiers joint, indivis ou pour lesquels le salarié « particulièrement sensible » dispose d'une procuration.
Les salariés « particulièrement sensibles » ne peuvent pas détenir des comptes d'instruments financiers sur lesquels ils agissent directement en passant eux-mêmes les instructions d'achat ou de vente de titres autres que ceux émis par des OPCVM.

Toutefois, les personnes qui possédaient préalablement à leur inscription sur la liste des salariés particulièrement sensibles un ou plusieurs comptes d'instruments financiers (ou qui s'en trouveraient titulaires indépendamment de toute initiative personnelle, à la suite d'une succession par exemple), ne sont pas contraintes à liquider immédiatement leurs positions. Dans ce cas, elles peuvent naturellement conserver les titres inscrits dans le ou les comptes d'instruments financiers mais :
- elles ne sont plus en mesure de procéder à l'acquisition de titres
- elles sont autorisées à céder leurs titres en informant de chaque opération réalisée le Responsable de la Conformité. Cette information est accompagnée d'une attestation sur l'honneur précisant que cette opération s'effectue en l'absence d'informations privilégiées.

Elles peuvent, le cas échéant, placer leur compte sous mandat de gestion et le déclarer au Responsable de la Conformité.

Les salariés « particulièrement sensibles » peuvent détenir des comptes d'instruments financiers investis uniquement en OPCVM.

Ils doivent satisfaire aux obligations suivantes :
- déclarer au Responsable de la Conformité les comptes titres investis uniquement en OPCVM ;
- communiquer les relevés d'opérations sur simple demande du le Responsable de la Conformité.

Les salariés « particulièrement sensibles » peuvent détenir des comptes titres sous mandat de gestion.

Ils doivent alors satisfaire aux obligations suivantes :
- déclarer au Responsable de la Conformité les comptes titres sous mandat de gestion
- communiquer une copie des relevés d'opérations sur simple demande du Responsable de la Conformité pour les Services d'Investissement (RSCI) de BPCE.

Les personnes « particulièrement sensibles » s'engagent à déclarer immédiatement au RCSI de BPCE toute nouvelle ouverture ou fermeture de comptes titres.

Article 6 : cadeaux et autres avantages

Selon les circonstances, les cadeaux d'affaire, les présents, les divertissements, les faveurs, les avantages et/ou les offres d'emploi peuvent s'avérer être des tentatives « d'acheter » ou d'obtenir par des moyens inappropriés des affaires, traitements de faveur ou avantages commerciaux. Accepter de tels avantages pourrait faire naître des doutes sur la capacité d'un salarié à porter un jugement indépendant dans le meilleur intérêt de la CEPAL.

6.1. Règles générales relatives aux cadeaux et autres avantages

Aucun membre du personnel ne doit accepter ou proposer -sous quelque forme que ce soit- de rémunération directe ou indirecte d'un client, d'un intermédiaire, d'un fournisseur ou d'un concurrent ou bien encore recevoir ou donner des libéralités ou invitations ou cadeaux.
Il peut cependant être admis que cette interdiction ne s'applique pas à tout cadeau, libéralités ou invitations reçu ou donné d'une valeur inférieure à celle communiquée par le Responsable de la Conformité, sauf à considérer que ceux-ci peuvent altérer le jugement professionnel du salarié ou risquer de le mettre en situation de conflit d'intérêts.

Toute dérogation au principe énoncé ci-dessus doit faire systématiquement l'objet d'une demande d'autorisation écrite auprès du supérieur hiérarchique. Celui-ci apprécie la suite à donner en fonction notamment des usages en vigueur.

Le principe de transparence exige par ailleurs que tout accord soit transmis (montant, nature, date, conditions, …) par le responsable hiérarchique au Responsable de la Conformité.
En cas de doute ou de difficulté, le salarié ou son supérieur hiérarchique recueille l'avis du Responsable de la Conformité de la CEPAL.

Article 7 : relations avec les clients, fournisseurs, prestataires ou intermédiaires

D'une manière générale, les salariés doivent, avant de communiquer à des clients, fournisseurs, prestataires ou intermédiaires le nom et/ou les coordonnées téléphoniques ou électroniques d'un salarié ou dirigeant de la CEPAL, s'assurer de son consentement préalable.

7.1. Relations avec les clients

En aucun cas un salarié ne peut accepter d'être désigné comme légataire ou donataire, ou bénéficiaire d'un contrat d'assurance vie d'un client autre qu'un membre de sa famille. S'il devait, à son insu, se trouver bénéficiaire de dons, notamment par le jeu d'une clause bénéficiaire stipulée à son profit ou le cas échéant par voie testamentaire et alors qu'aucun lien particulier ne peut justifier cette situation, il devra renoncer purement et simplement au capital décès.

Chaque salarié doit s'assurer de la connaissance de son client (identité, capacité, activité économique…). Il a un devoir d'information et de conseil vis-à-vis de son client et doit ainsi privilégier son intérêt en toutes circonstances.

Tout salarié doit s'interdire de négocier à titre personnel avec un client et servir d'intermédiaire entre des clients.

Tout salarié est tenu de ne pas solliciter ou bénéficier de prêts ou avances auprès des clients.

Tout salarié s'interdit de procéder à des opérations de démarchage au domicile de la clientèle sans être porteur d'une carte spéciale de démarchage et d'emploi qui doit lui être délivrée par son employeur. Il doit également respecter les dispositions légales et réglementaires spécifiques au démarchage en matière bancaire et financière.

7.2. Déontologie des salariés exerçant une activité professionnelle en lien avec des fournisseurs, prestataires ou intermédiaires

Les salariés exerçant des responsabilités professionnelles les mettant en contact avec des fournisseurs, prestataires ou intermédiaires extérieurs, s'interdisent d'accepter un avantage particulier qui pourrait leur être consenti par ces fournisseurs ou prestataires en vue de l'obtention d'un avantage commercial ou d'un traitement de faveur.
Les salariés concernés devront traiter tous les acteurs potentiels avec équité lors des consultations pour tous les achats importants sans exception et ne pas accepter, directement ou indirectement, cadeaux, distractions, rémunérations, bénéfices personnels ou autres gratifications d'aucune sorte de la part des fournisseurs existants ou potentiels.

Article 8 : Lutte contre le blanchiment de capitaux et le financement du terrorisme

La lutte contre le blanchiment des capitaux et le financement du terrorisme est une obligation légale qui s'impose à la CEPAL.

La CEPAL a adopté en conséquence des procédures spécifiques qui couvrent les obligations établies par le Groupe pour lutter contre le blanchiment de capitaux, le financement du terrorisme, la corruption et la criminalité.

Le délit de blanchiment est constitué par le fait d'apporter un concours à une opération de placement, de dissimulation ou de conversion du produit direct ou indirect d'un crime ou d'un délit. Il est puni de 10 ans d'emprisonnement et de 750 000 € d'amende lorsqu'il est commis de façon habituelle en utilisant les facilités que procure l'exercice d'une activité professionnelle.

Tout salarié doit refuser de prêter son concours à une opération de blanchiment de capitaux. En cas de doute il doit alerter dans les meilleurs délais, et si possible avant la réalisation de ladite opération, sa hiérarchie et/ou la Direction de la Conformité selon les procédures en vigueur au sein de l'entreprise et ne doit en aucun cas informer le client de sa démarche.

L'opération douteuse peut être définie comme une opération se présentant dans des conditions inhabituelles de complexité ou qui ne paraît avoir de justification économique ou d'objet licite, ou dont l'identité du donneur d'ordre ou du bénéficiaire reste incertaine malgré les diligences effectuées (article L 563-3 du code monétaire et financier).

Les responsables hiérarchiques doivent veiller chaque année à la formation de leurs salariés sur les matières de la prévention et de la lutte contre le blanchiment. Cette formation générale se double d'une information spécifique sur les normes du Groupe relatives à leur métier.

Article 9 : Lutte contre la fraude interne

La faculté d'alerte a par définition un caractère optionnel et s'exerce conformément à la procédure existante dans l'entreprise.

Les faits susceptibles de faire l'objet d'une alerte professionnelle, portent sur :

- un crime ou un délit ;
- une violation grave et manifeste :
  - d'un engagement international régulièrement ratifié ou approuvé par la France ;
  - d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un tel engagement ;
  - de la loi ou du règlement ;
- une menace ou un préjudice grave pour l'intérêt général ;
- l'existence de conduites ou de situations contraires au code de conduite de l'établissement ;
- une(des) opération(s) ou procédure(s) d'ordre strictement professionnel, conduisant à s'interroger sur l'existence éventuelle d'un dysfonctionnement dans la mise en œuvre effective des obligations de conformité auxquelles l'entreprise est soumise, c'est-à-dire susceptible d'engendrer un risque de non-respect des dispositions propres aux activités bancaires.

CAISSE D'EPARGNE
D'AUVERGNE ET DU LIMOUSIN

Annexe 3 : CHARTE D'UTILISATION DES MOYENS INFORMATIQUES ET DE COMMUNICATION ELECTRONIQUE

Article 1 : Préambule

La présente charte a pour objet de fixer les règles d'utilisation des moyens informatiques et de communication électronique mis à la disposition des utilisateurs dans le cadre de leur activité professionnelle.

Les règles ainsi définies sont destinées à assurer un usage des moyens informatiques et de communication électronique conforme à leur objet, ainsi qu'aux dispositions légales et réglementaires applicables.

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

La présente charte est rédigée dans le souci de concilier les intérêts de chaque utilisateur et ceux de la CEPAL. Elle manifeste ainsi la volonté de la CEPAL d'assurer un usage loyal, respectueux et responsable de ses moyens informatiques et de communication électronique, ainsi que de protéger son patrimoine et son image de marque.

La présente charte n'a pas pour objet et objectif de couvrir de façon exhaustive tous les cas de figure susceptibles de se présenter dans le cadre de l'utilisation des moyens informatiques et de communication électronique mis à la disposition des utilisateurs. C'est dans l'esprit des règles ainsi édictées que chacun devra se conformer dans des situations non envisagées.

La présente charte pourra évoluer en fonction du contexte légal et de la politique de sécurité notamment applicable au sein de la CEPAL.

Ces règles ont également pour objet d'atteindre un niveau optimum en termes de sécurité, de confidentialité et de performance dans l'usage de ces moyens.

Il appartient à l'utilisateur de se référer au document intitulé « livret technique », dont l'objet est de décliner au plan pratique les principes de mise en œuvre. Il s'agit d'un manuel d'utilisateur.

Article 2 : Portée et opposabilité

Conformément à l'article 13 du règlement intérieur, la présente charte est annexée à celui-ci et produit, à ce titre, les mêmes effets. En conséquence, l'utilisateur est réputé en avoir pris connaissance.

Article 3 : Champ d'application

3.1. Personnes concernées

La présente charte est applicable à toute personne autorisée à accéder aux moyens informatiques et de communication électronique, quel que soit leur statut (salariés, stagiaires,

intérimaires, mandataires sociaux, membres du Conseil d'Orientation et de Surveillance de la CEPAL, intervenants extérieurs tels que consultants, prestataires, sous-traitants, entreprises partenaires, travailleurs indépendants ou auditeurs, personnels détachés ou mis à disposition, etc.)

La présente charte est également applicable aux membres des instances représentatives du personnel et/ou titulaires d'un mandat syndical utilisateurs des moyens informatiques et de communication électronique mis à disposition par la CEPAL.

Toutefois, la présente charte pourra être complétée d'obligations spécifiques pour certaines catégories de personnel (notamment les administrateurs de systèmes d'informations).

3.2. Moyens concernés

SONT VISES PAR LA PRESENTE CHARTE :

- l'ensemble des moyens informatiques et de communication électronique qui sont la propriété de la CEPAL et/ou des sociétés du Groupe BPCE qui sont mis à la disposition des utilisateurs à des fins professionnelles ;

- l'ensemble des moyens informatiques et de communication électronique qui sont la propriété personnelle de l'utilisateur, et pour lesquels celui-ci a obtenu une autorisation d'utilisation dans le cadre de son activité professionnelle.

3.3. Usages concernés

Il est rappelé que l'usage des moyens informatiques et de communication électronique s'inscrit notamment dans le respect de la Loi, de la sécurité de la CEPAL et du bon usage, gages d'efficacité opérationnelle. La négligence et la mauvaise utilisation des ressources font courir des risques à l'entreprise.

La présente charte s'applique à tous les types d'usage des moyens informatiques et de communication électronique qu'ils aient lieu :
- dans les locaux de la CEPAL, principalement dans les sites administratifs et les agences bancaires ;
- dans le cadre d'un usage dit « nomade », quel qu'en soit le lieu ;
- dans le cadre d'un accès distant, quelque soit le lieu de cet accès (domicile, etc.)

La présente charte s'applique quelles que soient la fréquence et la périodicité de l'utilisation des moyens informatiques et de communication électronique.

Article 4 : Conditions d'utilisation

4.1. Usage professionnel

Les moyens informatiques et de communication électronique sont réservés à un usage professionnel (comprenant l'usage qui pourrait en être fait par les membres des instances représentatives du personnel et/ou titulaires d'un mandat syndical dans le cadre de l'exercice de leur mandat), quel que soit le lieu où l'activité est exercée.

En particulier, l'adresse électronique est strictement professionnelle.

Sa communication est réservée à des correspondances professionnelles. Elle ne doit donc pas être utilisée dans un autre contexte, et notamment diffusée sur des sites internet (chats, forums, blogs, etc.), sans rapport avec l'activité professionnelle.

L'inscription sur des listes de diffusion permettant la réception automatique et périodique d'informations est également réservée à un usage strictement professionnel.

L'inscription sur des listes de diffusion est basée sur un principe d'autodiscipline des utilisateurs, destiné à s'assurer d'une part, de la pertinence et de la nécessité d'une telle inscription et d'autre part, des conséquences de celle-ci (fréquence de réception des messages, poids des messages, encombrement des réseaux, etc..).

L'accès à des services en ligne (sites web, blogs, forums, chats, etc.) est également strictement réservé à un usage professionnel.

Dans tous les cas, et quelles que soient les conditions effectives d'utilisation, l'usage des moyens informatiques et de communication électronique est présumé avoir un caractère professionnel.

Aux termes de la jurisprudence, sont ainsi présumés avoir un caractère professionnel, notamment :
- les fichiers créés grâce à ces moyens (voir §3.2) par un utilisateur, pour l'exécution de son travail ou de ses activités de représentation du personnel, sauf lorsque celui-ci les identifie comme étant personnels ;
- les connexions établies par un utilisateur sur des sites internet pendant son temps de travail grâce à un moyen informatique ou de communication électronique, pour l'exécution de son travail ou de ses activités de représentation du personnel.

Il en résulte que la CEPAL peut y accéder hors de la présence de l'utilisateur.

4.2. Usage non professionnel

Bien que les moyens informatiques et de communication électronique soient réservés à un usage professionnel, leur utilisation à des fins non professionnelles, pour répondre en cas d'urgence à des obligations socialement admises, est tolérée.

L'usage des moyens informatiques et de communication électronique se traduit dans les faits par :
- la possibilité de créer un répertoire informatique non professionnel ;
- la possibilité d'utiliser l'adresse électronique à des fins non professionnelles.

Cette tolérance s'inscrit dans le strict respect des règles ci-après :

✶ Cet usage doit donc être exceptionnel et demeurer raisonnable.

✶ Un tel usage ne doit pas :
− perturber le bon fonctionnement des moyens informatiques et de communication électronique, du service et de la CEPAL en général,
− compromettre ses activités ou opérations commerciales,
− ne doit en aucun cas porter atteinte ou être susceptible d'engager la responsabilité de la CEPAL,
− poursuivre un but lucratif ou même ludique.

∗ La confidentialité attachée au répertoire informatique est conditionnée par le fait que ce répertoire soit clairement identifiable en tant que tel.

∗ Le répertoire informatique privé, utilisé pour stocker des documents personnels, doit être identifié par le terme : « PRIVE », sa localisation étant spécifiée dans le livret technique.

∗ Tous les répertoires informatiques autres que le répertoire identifié comme « PRIVE », sont considérés comme professionnels.

∗ Ce stockage doit, de la même manière que pour tout usage non professionnel des moyens informatiques et de communication électronique mis à disposition par la CEPAL, répondre en cas d'urgence à des obligations socialement admises. Il doit donc demeurer exceptionnel et raisonnable. Lesdites obligations disparues, les fichiers du répertoire informatique identifié par le terme « PRIVE » doivent être supprimés ou transférés sur tous moyens personnels par l'utilisateur concerné.

∗ Aucune information à caractère professionnel ne peut être ni stockée dans le répertoire informatique « PRIVE » de sa messagerie électronique, ni émise ou reçue via le courrier électronique identifié comme « PRIVE ».

∗ Il est rappelé que l'adresse électronique professionnelle –prénom.nom@cepal.caisse-epargne.fr– est strictement réservée à un usage professionnel

∗ Néanmoins pour répondre à des besoins à caractère d'urgence et à titre exceptionnel, l'utilisateur peut émettre ou recevoir des courriers électroniques non professionnels sur son adresse électronique professionnelle, la confidentialité attachée à la correspondance professionnelle implique la notion du terme « PRIVE » dans la zone « objet du message ». La perspective d'une réponse impose d'informer le tiers destinataire du message de cet usage.

∗ Tout courrier électronique adressé ou reçu à partir de l'adresse électronique professionnelle – prénom.nom@cepal.caisse-epargne.fr ne portant pas mention « PRIVE » est considéré comme professionnel.

∗ Lorsque le moyen de communication utilisé ne comporte pas de champ « objet » (chat, messagerie instantanée, ..), le message à caractère personnel doit débuter par le terme [PRIVE].

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

∗ L'usage des moyens informatiques et de communication électronique à des fins non professionnelles relève de la seule et entière responsabilité de l'utilisateur, qui dégage en conséquence la CEPAL de toute responsabilité.

∗ Le caractère non professionnel de l'usage des moyens informatiques et de communication électronique interdit, par principe, à la CEPAL d'accéder aux contenus ou données émis, reçus ou échangés dans ce cadre.

∗ Le caractère « non professionnel » du répertoire ou des courriers électroniques échangés, ne fait pas obstacle à ce que :

- la CEPAL puisse accéder de manière exceptionnelle à ces éléments lorsqu'il existe un risque avéré pour l'entreprise en termes notamment de sécurité, de continuité de service, ou un risque grave de voir sa responsabilité engagée ;

- ces éléments fassent l'objet de conservation technique dans le cadre des procédures de back up ou de plans de continuité ou reprise d'activité mises en œuvre au sein de la CEPAL ;

- en cas de détection ou de suspicion de la présence d'un code malveillant à la mise en quarantaine ou le cas échéant, à la suppression de l'élément quelconque qui comporte ou comporterait un code malveillant ;

- un administrateur ou toute personne « habilitée », accède à ces contenus dans le cadre de sa mission consistant à assurer le fonctionnement normal et la sécurité des moyens informatiques et de communication électronique, ce notamment dans le cadre d'opération de maintenance *(cf. fiche n°7 du rapport pour les employeurs et les salariés 2008 de la Cnil, « les administrateurs ont pour mission d'assurer le fonctionnement normal et la sécurité des réseaux et systèmes. Ils sont conduit par leurs fonctions mêmes à avoir accès à des informations personnelles relatives aux utilisateurs (messagerie, historique des sites visités, fichiers « LOGS » ou de journalisation, etc.) y compris celles qui sont enregistrées sur le disque dur du poste de travail (fichiers temporaires, cookies) » ;*

- la CEPAL puisse, dans tous les autres cas, et pour des motifs légitimes, accéder à ces éléments en présence de l'utilisateur ou ce dernier dûment appelé, ou, en son absence, dès lors qu'elle y est autorisée par une décision de justice ou une autorité habilitée à cet effet (police, gendarmerie, douanes, Cnil, Direction générale de la concurrence, de la consommation et de la répression des fraudes, etc.).

Article 5 : Conditions d'accès et d'identification

Chaque utilisateur est doté d'un ou de plusieurs identifiants permettant l'accès aux moyens informatiques et de communication électronique.

L'identifiant peut prendre diverses formes (login/password, biométrie, signature électronique, token sur une clé USB ou bien une carte avec ou sans contact, etc.).

Les utilisateurs sont informés que la CEPAL pourra mettre en place des moyens d'identification par biométrie et elle déterminera s'il y a lieu les conditions de mise en œuvre.

L'identifiant est dans tous les cas personnel, et confidentiel.

Il est dès lors interdit à l'utilisateur de :
- procéder à la moindre divulgation, même intra-service, de son ou de ses identifiant(s) ;
- d'utiliser un identifiant autre que le sien, dans l'hypothèse où il en aurait eu connaissance ;
- de supprimer, masquer ou modifier son identité ou son identifiant ;
- si par erreur ou suite à un dysfonctionnement l'utilisateur accède à des informations, des traitements ou des systèmes internes ou externes qui ne lui sont pas autorisées, il s'engage à ne pas s'y maintenir et doit sans délai en informer sa hiérarchie et le signaler auprès du service d'assistance informatique.

Si ces identifiants, par nature confidentiels, ont fait l'objet d'une communication ou qu'il existe un risque qu'ils aient été communiqués, ou encore s'ils ont été oubliés, l'utilisateur concerné doit, selon la procédure mise en place par la CEPAL, renouveler ses identifiants. S'il existe une difficulté à ce renouvellement, ce dernier doit se rapprocher du service d'assistance informatique.

L'identifiant doit être modifié selon une fréquence déterminée et fixée le cas échéant dans le livret technique.

Lorsqu'un accès à distance est accordé à un utilisateur, celui-ci s'engage à utiliser, à l'exclusion de tout autre, les moyens techniques d'authentification qui lui seront remis.

Lors de l'utilisation d'un accès distant, en termes de sécurité et de confidentialité, l'utilisateur est soumis aux mêmes obligations que celles visées pour la gestion des identifiants et devra suivre toutes les prescriptions complémentaires qui lui seront signifiées.

L'utilisateur d'un accès distant devra aviser, sans délai, les services compétents de la perte ou du vol des moyens d'authentification à distance. Il devra également, selon les cas, soit assister la CEPAL, soit procéder lui-même à toutes les démarches (déclaration d'assurance, dépôt de plainte, etc.) rendues nécessaires à la suite d'un incident de quelque nature que ce soit.

La suppression et la suspension d'autorisation d'accès aux moyens informatiques et de communication électronique font l'objet d'une description dans le livret technique.

Sauf à avoir engagé préalablement une demande de suspension ou de suppression d'autorisation, ou à être en mesure de démontrer le contraire, tout usage des moyens informatiques et de communication électronique est réputé avoir été réalisé par le bénéficiaire de l'identification d'accès qui en assume toutes conséquences, notamment juridiques et financières.

La CEPAL se réserve, pour quelque raison que ce soit, de manière temporaire ou définitive, le droit d'accorder, de refuser, de modifier ou de supprimer en tout ou partie, le droit d'accès de toute personne aux moyens informatiques et de communication électronique.
Elle s'efforcera, autant que faire se peut, de prévenir l'utilisateur concerné dans des délais raisonnables, notamment en cas de maintenance.

Article 6 : Mobilité

Dans le cadre de ses déplacements professionnels, quelle que soit leur durée ou leur fréquence, l'utilisateur assure la garde et la responsabilité des moyens informatiques et de communication électronique.

Cet usage de moyens informatiques et de communication électronique dits « nomades » impose à l'utilisateur un niveau de surveillance et de confidentialité renforcée.

En particulier, l'utilisateur se doit d'adopter une attitude de prudence et de réserve au regard des informations et des ressources du système d'information de la CEPAL qu'il pourrait être amené à manipuler ou à échanger.

Il doit également veiller à ce que des tiers non autorisés ne puissent accéder à ces moyens, les utiliser ou accéder à leurs contenus.

En cas non seulement d'incident avéré mais également de doute, l'utilisateur doit immédiatement en aviser la CEPAL.

Les utilisateurs sont informés que l'utilisation de matériel nomade fait l'objet d'une connexion aux systèmes d'information par un canal de communication particulier et que les accès sont tracés et consultables par les personnes effectuant les opérations de contrôles et d'audit.
Il est rappelé que les utilisateurs (à l'exception des salariés en période d'astreinte) ne sont pas tenus d'utiliser des moyens informatiques ou de communication électronique permettant de travailler à distance pendant leurs jours et heures de repos. Les salariés n'ont, à cet égard, aucune obligation de répondre à une communication électronique pendant leurs jours de repos, sauf événement urgent et exceptionnel.

Article 7 : Télétravail

La CEPAL déterminera, s'il y a lieu, les conditions de mise en œuvre du télétravail et pourra pour ce faire prévoir ou ajouter des règles spécifiques à la présente charte.

Article 8 : Utilisation des outils personnels à des fins professionnelles

La CEPAL n'autorise pas par principe l'utilisation des outils personnels à des fins professionnelles.

Dans le cas où la CEPAL déciderait d'autoriser l'utilisation d'outils personnels à des fins professionnelles, alors des règles spécifiques seront ajoutées à la présente charte.

Article 9 : Gestion des absences et des départs

Chaque utilisateur doit veiller à ce que la continuité du service soit assurée, conformément aux modalités d'organisation définies par la CEPAL.

Il n'est pas prévu de recourir à l'utilisation d'automatisme de gestion de messagerie électronique, ni de procédure spécifique en cas d'absence de lecture des messages au-delà d'un certain délai.

En cas d'absence, les utilisateurs doivent cependant activer leur message d'absence, ou à défaut cette action sera réalisée par le supérieur hiérarchique de l'utilisateur, ou bien demandée par ce dernier au service d'assistance informatique en tant qu'action de maintenance.

Certains utilisateurs peuvent paramétrer leur messagerie afin que celle-ci soit déléguée et ce notamment en cas d'absence.

En cas d'absence de l'utilisateur, pour quelque raison et durée que ce soit, la CEPAL se réserve le droit d'accéder directement aux différents dossiers, répertoires, courriers électroniques et plus généralement tous documents à caractère professionnel de l'utilisateur.

A l'annonce du départ de la CEPAL d'un utilisateur, et pour des raisons légitimes de protection de ses intérêts, les droits d'accès et les conditions d'utilisation des moyens informatiques et de communication électronique seront modifiés. De même, des règles particulières de traçabilité pourront être mises en œuvre.

Lors de son départ, l'utilisateur doit remettre en bon état général de fonctionnement l'ensemble des moyens informatiques et de communication électronique qui lui ont été remis et les restituer.

Ses identifiants sont désactivés et le compte d'accès principal est supprimé selon le délai défini au niveau de la communauté informatique du Groupe. La suppression entraine la suppression de tous les fichiers associés (sauf dans les sauvegardes).

Si l'utilisateur a bénéficié d'un moyen d'authentification à distance, il s'engage à le restituer.

Le répertoire nommé « PRIVE », ainsi que tous les messages électroniques de même nature, doivent être supprimés par l'utilisateur au plus tard la veille de son départ de la CEPAL.

A défaut, et sauf procédure judiciaire ou enquête administrative, ces éléments sont automatiquement supprimés après le départ de l'utilisateur de la CEPAL selon le délai défini au niveau de la communauté informatique du Groupe, sans être consultés et sans qu'aucune copie ne soit réalisée.

Article 10 : Espaces collaboratifs

La CEPAL a mis en place des espaces collaboratifs de travail.

La qualité des informations disponibles est un objectif élevé. Aussi, chaque utilisateur s'engage à être attentif à la pertinence des informations diffusées au sein de ces espaces et à travers les outils de gestion mis à sa disposition.

Par souci de qualité, de responsabilité et de protection du patrimoine informationnel de la CEPAL, l'utilisation de ces mêmes espaces et outils peut faire objet d'opérations de contrôle, d'audit, de modération et de traçabilité renforcées.

Article 11 : Réseaux/Medias sociaux

L'utilisation des réseaux sociaux peut être source de risques et de responsabilité notamment en termes d'image, de fraude, d'intelligence économique et de concurrence déloyale. Aussi, afin de limiter les risques encourus, les règles suivantes ont été arrêtées.

11.1. Usage du ou des réseaux/médias sociaux de l'entreprise

La CEPAL considère que les réseaux sociaux d'entreprise, les web TV d'entreprise et les services de type podcast permettent de partager des informations utiles au développement des produits, à l'amélioration du service fourni et à l'innovation.

A ce titre, le Groupe BPCE et la CEPAL peuvent développer des réseaux sociaux internes.

Les administrateurs du réseau social désignent les personnes responsables de la supervision de l'activité générée sur le réseau social. Ces responsables ont notamment pour mission de superviser les profils d'utilisateurs, les publications diffusées et les groupes créés sur le réseau social. Dans ce cadre, l'administrateur du réseau dispose du pouvoir de supprimer ou de suspendre le profil d'un utilisateur, une publication ou un groupe, s'il constate un manquement à une règle visée ou prévue dans la présente charte.

Les modalités d'accès et d'inscription sont définies dans les Conditions Générales d'Utilisation (CGU) du réseau social et s'imposent aux utilisateurs, qui reconnaissent les avoir acceptées expressément et sans réserve lors de leur inscription.

Les utilisateurs veilleront à l'exactitude des informations les concernant dans le cadre de la création et de la mise à jour de leur profil (nom, prénom, profession, coordonnées …). Ces données pourront être modifiées ou supprimées librement par l'utilisateur.

Compte tenu de la liberté et de la facilité d'accès au réseau social d'entreprise, les utilisateurs sont seuls responsables de la fréquence et des horaires auxquels ils s'y connectent. Compte tenu de la finalité professionnelle du réseau social d'entreprise, toute connexion en dehors des horaires habituels de travail relève de la seule initiative des utilisateurs.

Les utilisateurs s'engagent à contribuer à assurer un bon fonctionnement du réseau social, en s'abstenant de détourner une ou plusieurs de ses fonctionnalités de son usage normal ou de l'utiliser pour envoyer massivement des messages non sollicités aux autres utilisateurs.

D'une manière générale, les utilisateurs s'engagent à ne pas apporter volontairement des perturbations au bon fonctionnement des systèmes informatiques et du réseau de l'entreprise, que ce soit par des manipulations anormales, ou par l'introduction de logiciels parasites connus sous le nom générique de virus, chevaux de Troie, …

Il est interdit d'extraire, de stocker, de reproduire, de représenter ou de conserver, directement ou indirectement, sur un support quelconque, par tout moyen et sous toute forme que ce soit, tout ou partie qualitativement ou quantitativement substantielle des contacts auquel l'utilisateur accède à titre professionnel.

Enfin, il est rappelé que les moyens de communication des instances représentatives du personnel et des organisations syndicales sont définis conventionnellement. Le ou les réseaux sociaux de l'entreprise ou du groupe n'ont pas vocation à se substituer à cette fin.

Les profils, publications ou groupes qui ne respectent pas ces règles pourront être supprimés ou suspendus à tout moment par les administrateurs du réseau social.

Les utilisateurs pourront signaler tout contenu leur semblant contraire à ces règles aux administrateurs du réseau social. Pour cela, les utilisateurs sont invités à prendre contact avec la Direction de l'entreprise en charge de l'administration du réseau.

Les profils des utilisateurs et les informations qu'ils contiennent sont librement accessibles par les autres utilisateurs du réseau social.

La réglementation relative à la protection des données personnelles (loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ainsi que le règlement européen n°2016/679 du 26 avril 2016 dit Règlement Général sur la Protection des Données), définissent les conditions dans lesquelles des traitements de données personnelles peuvent être opérés. Ils instituent, au profit des personnes concernées par les traitements, des droits que la présente charte invite à respecter, tant à l'égard des utilisateurs que des tiers.

Des traitements de données automatisés et manuels sont effectués conformément à la présente charte. Ils sont, en tant que de besoin, déclarés conformément à la loi du 6 janvier 1978.

Les données collectées dans le cadre de la gestion du réseau social d'entreprise sont destinées à l'usage exclusif des personnes habilitées pour l'exercice de leurs missions. Elles sont à usage purement interne et ne font l'objet d'aucune communication, cession ou divulgation à des tiers.

L'utilisateur est responsable de tous les éléments permettant l'accès sécurisé au réseau social. En aucun cas, ces données ne devront être communiquées à des tiers.

11.2. Usage du ou des réseaux/médias sociaux externes

La CEPAL estime que les réseaux sociaux extérieurs à l'entreprise occupent une place grandissante dans la vie des affaires. Ces réseaux permettent à ses salariés de créer de nouvelles relations avec ses clients et partenaires et d'optimiser la communication commerciale autour de ses produits.

L'entreprise entend exploiter dans les meilleures conditions les nombreuses opportunités offertes par le développement des médias sociaux permettant d'interagir avec ses salariés et avec le public (Facebook, Twitter, LinkedIn, Youtube, Yammer…).

A cet égard, tout en souhaitant profiter du potentiel offert par ces nouveaux modes de communication, l'entreprise souhaite se prémunir au mieux contre les risques liées à une mauvaise utilisation des médias sociaux.

Dans le cadre de l'utilisation des médias sociaux par ses salariés, l'entreprise entend se conformer aux règles en vigueur, résultant notamment de la recommandation n°2016-R-01 de l'ACPR sur l'usage des médias sociaux à des fins commerciales, en date du 14 novembre 2016.

Seuls les salariés ou mandataires sociaux qui y sont expressément autorisés peuvent communiquer au nom ou pour le compte de l'entreprise sur les médias sociaux, définis comme l'ensemble des technologies permettant l'interaction sociale et la création de contenus collaboratifs sur internet y compris via des applications mobiles : blogs, réseaux sociaux, forums de discussion, cette liste n'étant pas exhaustive.

Ces personnes autorisées bénéficient à cette fin d'un compte professionnel distinct de leurs comptes privés, créé par l'entreprise. Ce compte sera identifié de manière à reconnaître clairement le caractère professionnel des comptes utilisés sur les médias sociaux.

Le compte professionnel est le seul par le biais duquel les personnes autorisées peuvent communiquer au nom ou pour le compte de l'entreprise.

Dans le cadre de leur activité sur les médias sociaux, ces personnes veilleront à ce que le contenu diffusé, entendu comme une communication à caractère publicitaire ou comme une communication ayant pour objectif la conclusion d'un acte de vente ou une incitation à l'achat, quelle qu'en soit la forme (messages, allégations, photos ou vidéos), soit conforme à la réglementation et notamment présenté de manière loyale et claire.

Les personnes autorisées utiliseront uniquement les outils de communication de l'entreprise, selon les instructions qui leur ont été données. Il est à cet égard expressément rappelé que la diffusion de tout support de communication commercial est préalablement soumise au respect des procédures de validation interne (service communication commerciale, direction Juridique, direction de la Conformité…). La diffusion d'un support déjà existant, quelle qu'en soit la forme antérieure (papier, format électronique…) est prohibée, sauf à obtenir préalablement l'accord commun des directions précitées.

En cas de doute sur l'utilisation d'un réseau social, l'utilisateur devra immédiatement consulter sa hiérarchie.

L'autorisation donnée pourra être retirée, modifiée ou suspendue dès lors que l'intérêt de l'entreprise le justifie.

La personne autorisée devra prendre toutes les précautions utiles pour que son utilisation des réseaux sociaux soit sans danger pour les systèmes d'information de l'entreprise.

Les personnes qui n'y sont pas expressément autorisées ne sauraient en aucune manière s'exprimer, de quelque façon que ce soit, et sur quelque média social que ce soit, au nom ou pour le compte de l'entreprise.

11.3. Règles d'usage professionnel et non-professionnel

Usage professionnel

Chaque utilisateur est responsable civilement et pénalement du contenu qu'il publie sur les réseaux sociaux. Il peut librement supprimer ses propres messages.

L'utilisateur devra s'abstenir de publier un contenu de façon anonyme et, au contraire, s'identifier clairement, en précisant sa fonction au sein de l'entreprise.

Il est interdit de publier sur le réseau social des informations sensibles ou confidentielles, relatives notamment à la clientèle, à l'organisation, au fonctionnement et aux modes de gestion des ressources de l'entreprise et du groupe auquel elle appartient.

Les publications devront présenter un lien avec l'environnement professionnel et respecter les lois et règlements en vigueur, les droits des tiers et de la propriété intellectuelle, le Règlement Intérieur de l'entreprise, la présente Charte (le cas échéant), les éventuelles dispositions résultant du contrat de travail, la politique générale de sécurité de l'entreprise.

De même, les publications ne devront pas revêtir de caractère politique, religieux, idéologique ou contraire à l'esprit du réseau social. Elles ne devront pas non plus poursuivre des fins commerciales ou promotionnelles autres que celles de l'objet social de l'entreprise.

Les utilisateurs devront répondre aux contributions des tiers avec pertinence, exactitude, et ne pas porter atteinte à l'image de marque de l'entreprise

Les utilisateurs devront faire preuve de modération, de courtoisie et de respect dans le cadre de l'utilisation du réseau social, vis-à-vis tant des autres utilisateurs que des autres salariés et entreprises du groupe BPCE. Les publications à caractère discriminatoire, injurieux, pornographique, obscènes, diffamatoires, violents ou racistes sont strictement interdites.

Les utilisateurs veilleront à respecter le droit à la vie privée et à l'intimité des personnes dans le cadre de leurs publications sur le réseau social.

Les utilisateurs qui ne respectent pas les règles prévues ou visées dans la présente charte s'exposent à des sanctions disciplinaires en application du présent règlement intérieur de l'entreprise.

Usage non professionnel

Dans le cadre de la sphère non professionnelle et hors les murs de l'entreprise, le salarié est bien évidemment libre d'utiliser les réseaux sociaux. Cependant il reste tenu de respecter les principes de confidentialité et de secret applicables à son activité professionnelle. Il lui est ainsi interdit de diffuser toute information relevant du secret bancaire ou du secret des affaires, en particulier les informations confidentielles, les informations commerciales sensibles relatives à l'entreprise, ses salariés, ses clients, ses partenaires ou ses concurrents.

En tout état de cause, le salarié s'interdit de publier des contenus portant atteinte à l'image et la réputation de l'entreprise, des salariés, des clients, partenaires ou concurrents de l'entreprise.

Article 12 : Protection de la propriété intellectuelle

L'utilisation des moyens informatiques et de communication électronique de la CEPAL implique le respect des droits de propriété intellectuelle.

Sans que cette liste soit exhaustive, l'utilisateur est tenu :

- d'utiliser les logiciels, applications, dans les conditions de la licence souscrite par la CEPAL ;

- de ne pas effectuer de copie illicite de logiciel, d'applications et, a fortiori, de tenter d'installer des logiciels pour lesquels la CEPAL ne possèderait pas un droit d'usage ;

- de ne pas reproduire et utiliser les bases de données, pages web ou autres créations de la CEPAL ou de tiers protégés par le droit d'auteur ou un droit privatif sans avoir obtenu préalablement l'autorisation du titulaire de ces droits ;

- de ne pas diffuser des textes, des images, des photographies, des œuvres musicales ou audiovisuelles et, plus généralement, toute création copiée sur le réseau internet ;

- de ne pas copier et remettre à des tiers des créations appartenant à des tiers ou à la CEPAL sans s'assurer de l'autorisation du titulaire des droits qui s'y rapporte.

Les utilisateurs sont soumis aux règles du droit d'auteur et du « Copyright » en matière d'utilisation des logiciels propriété de la CEPAL.

Article 13 : Préservation du secret et de la confidentialité

Les informations secrètes sont protégées aux termes de la Loi et les informations confidentielles sont protégées en application d'une convention. Le caractère confidentiel de ces dernières informations résulte donc de la volonté des parties.

Il est rappelé aux utilisateurs qu'ils sont soumis au secret professionnel et à la confidentialité la plus stricte à l'égard de toute information non publique dont il pourrait avoir connaissance quelle qu'en soit la source, dès lors qu'elle a été obtenue dans le cadre de l'activité professionnelle *(cf. articles 1 et 2 de l'annexe 2 du Règlement Intérieur : Charte de Conformité et de Déontologie.)*

Le respect de cette obligation implique notamment de :

- veiller à ce que les tiers non autorisés n'aient pas connaissance de telles informations ;
- n'accéder qu'aux informations en rapport direct avec sa fonction et ne pas chercher, en conséquence, à prendre connaissance d'informations réservées à d'autres utilisateurs ;
- d'une manière générale, respecter les règles d'éthique professionnelle, de déontologie, ainsi que les obligations de réserve et devoir de discrétion en usage au sein de la CEPAL.

L'attention de l'utilisateur est attirée sur les risques liés à la diffusion de contenus d'information sur internet, en particulier au sein des réseaux sociaux et sur les blogs. Il est donc strictement interdit de diffuser la moindre information à caractère professionnel, qu'elle soit ou non protégée par une obligation légale de secret ou une obligation contractuelle de confidentialité sur internet.

La diffusion de toute donnée ne peut être réalisée qu'aux conditions suivantes :
- habilitation de l'émetteur ;
- désignation d'un destinataire autorisé ;
- respect d'une procédure sécurisée.

L'utilisation de procédés de cryptage est une fonction qui ne peut être mise en œuvre que dans certains cas autorisés. Il est interdit d'utiliser des moyens de cryptologie autres que ceux expressément autorisés par la CEPAL.

Article 14 : Protection des données à caractère personnel

14.1. Devoirs des utilisateurs

Les utilisateurs sont informés de la nécessité de respecter les dispositions légales en matière de traitements automatisés ou manuels de données à caractère personnel. Ces dispositions figurent pour l'essentiel dans la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite loi « Informatique et libertés ».

Toute constitution de fichiers ou de bases de données comprenant des données à caractère personnel devra être portée à la connaissance de la Hiérarchie et du Directeur de la Conformité avant de faire l'objet de formalités préalables auprès de la Cnil, sauf dérogations légales ou réglementaires.

La diffusion de données à caractère personnel à l'attention de tiers extérieurs à la CEPAL doit se faire en prenant toutes les précautions utiles, notamment pour préserver la sécurité des informations transmises, et s'assurer que cette diffusion est autorisée.

14.2. Droits des utilisateurs

La CEPAL s'engage à ce que les données concernant les utilisateurs soient collectées et traitées de manière loyale et licite, dans les conditions exposées.

Les traitements opérés dans le cadre de la présente charte ont pour finalité :
- le suivi et la maintenance des moyens informatiques et de communication électronique, qu'il s'agisse des applications informatiques internes ou des accès vers l'extérieur (soit notamment l'accès à internet) ;
- la gestion des annuaires permettant de définir les autorisations d'accès aux applications et réseaux ;
- la mise en œuvre de dispositifs destinés à assurer la sécurité et le bon fonctionnement des moyens informatiques et de communication électronique, notamment la conservation des logs de connexion et des données de toute nature ;
- la gestion de la messagerie électronique ;
- le fonctionnement en réseaux internes par métiers ou par projet permettant la collecte, la diffusion ou la traçabilité de données de gestion des tâches, de la documentation, de la gestion administrative et des agenda des personnes répertoriées dans ces réseaux ;
- le respect de la présente charte.

Conformément à la loi « Informatique et libertés », les utilisateurs sont informés, en particulier, qu'ils disposent d'un droit d'accès, de rectification et d'opposition, pour motif légitime, relatif à l'ensemble des informations à caractère personnel les concernant, et qui s'exerce auprès du Responsable de la Conformité.

Article 15 : Sécurité

Les moyens informatiques et de communication électronique sont exclusivement installés, configurés et paramétrés par le personnel habilité par la CEPAL.

Lorsqu'il s'agit de moyens personnels à l'utilisateur, ceux-ci sont nécessairement autorisés voire contrôlés par ce même personnel.

A des fins de précaution, certaines configurations peuvent être verrouillées par la CEPAL (poste de travail, accès internet, etc.).

La mise en place d'outils de sécurité par la CEPAL ne doit pas, toutefois, dispenser les utilisateurs d'une obligation de vigilance à cet égard.

En effet, tout utilisateur a la charge, à son niveau, de contribuer à la sécurité des moyens informatiques et de communication électronique mis à sa disposition, principalement en évitant l'introduction de codes malveillants susceptibles d'endommager le système d'information de la CEPAL.

Cette vigilance passe notamment par le respect des règles de conduite suivantes :
- ne pas ouvrir les pièces jointes reçues de l'extérieur quand l'émetteur du message est inconnu ou douteux ;
- détruire les messages du type « chaîne de solidarité » ;
- ne pas stocker et router des gadgets reçus ou trouvés sur internet ;
- ne pas faire suivre les messages d'alerte de l'arrivée d'un virus mais prévenir la Direction des systèmes d'information.

En cas de réception de messages non sollicités (spams), l'utilisateur veille à :
- ne pas l'ouvrir ;
- ne pas y répondre ;
- ne pas le transférer ;
- informer le Responsable de la Sécurité des Systèmes d'Informations (RSSI) en cas de spam intrusif ;

En cas d'incitation à communiquer des informations sur les moyens informatiques et de communication électronique mis à disposition, ou bien à demander à intervenir sur le poste de l'utilisateur, ce dernier se doit de :
- vérifier la légitimité du demandeur ;
- ne pas donner suite en cas de doute et avertir immédiatement le RSSI.

L'utilisateur s'interdit également de :
- modifier les moyens mis à sa disposition notamment par l'ajout de logiciels, progiciels, même gratuits, 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 la Direction de l'Organisation et des Systèmes d'Information après validation de sa hiérarchie ;
- modifier ou détruire, ou tenter de modifier ou détruire, des fichiers sur lesquels il ne dispose d'aucun droit, en particulier les fichiers contenant des informations comptables ou d'identification ;
- mettre à la disposition d'utilisateurs non autorisés un accès aux systèmes ou aux réseaux à travers les matériels dont il a usage ;
- utiliser ou tenter d'utiliser des comptes autres que ceux qui lui sont attribués ou masquer son identité ;
- effectuer des opérations pouvant nuire aux relations internes ou externes de la CEPAL.

D'une manière générale, toute installation ou utilisation de matériels non expressément autorisée par la Direction des systèmes d'information est interdite.

L'utilisateur ne doit pas concevoir et/ou mettre en place des automatismes obéissants à un langage informatique (exemples : VBA, MS Access, …) programmé par lui-même, sauf si ces

programmations font partie du métier de l'utilisateur ou s'il en a reçu l'autorisation de sa hiérarchie.
Le manager qui autorise un salarié à réaliser un tel développement assume les responsabilités du résultat produit, notamment en termes de sécurité. Il mettra en œuvre les parades nécessaires à couvrir les risques induits.

L'utilisateur est tenu d'informer, sans délai, la CEPAL de tout dysfonctionnement, altération, perte, vol, destruction et autre événement pouvant affecter les moyens informatiques et de communication électronique. Il est tenu, en particulier, de signaler toute tentative d'intrusion extérieure, de falsification ou de présence de virus au département informatique de la CEPAL, ainsi qu'au RSSI.

La CEPAL, en tant qu'acteur économique, est un opérateur d'importance vitale et est soumise à des obligations particulières en termes de sécurité et notamment aux recommandations du Groupe BPCE en termes de sécurité du système d'informations. Afin de garantir la sécurité du système d'information, la CEPAL a recours au filtrage d'URL et au déchiffrement de certains sites internet dans le respect de la loi Informatique et Libertés.

Article 16 : Traçabilité et filtrage

Pour satisfaire aux obligations légales qui lui incombent, tenant à sa capacité à :
- apporter la preuve, le cas échéant, du bon usage des moyens informatiques et de communication électronique mis à la disposition des utilisateurs ;
- à prévenir tout usage illicite de ces mêmes moyens.

La CEPAL procède à la mise en place :
- d'outils de traçabilité (journaux de connexions) de l'ensemble des moyens informatiques et de communication électronique ;
- d'outils de filtrage (filtrage des contenus, des URL, protocolaire, etc.) permettant d'analyser les conditions d'utilisation de ces moyens, d'interdire tel ou tel protocole, ou encore de restreindre ou d'interdire l'accès à internet ou à certaines catégories de sites internet.

Il est précisé que ces outils, en ce qu'ils portent entre autre sur l'accès à internet, permettent un contrôle des connexions des utilisateurs aux webmails, réservés exclusivement à la consultation de leur messagerie électronique personnelle.

Tout détournement, altération ou modification de ces outils ou des données recueillies grâce à ces outils est strictement interdit.

Article 17 : Maintenance

La mise à disposition des moyens informatiques et de communication électronique implique nécessairement des opérations de maintenance technique, qu'il s'agisse de maintenance corrective, de maintenance préventive ou de maintenance évolutive.

L'objectif de ces opérations n'est autre que d'assurer le bon fonctionnement et la sécurité des systèmes d'information. Elles se distinguent en cela des opérations de contrôle et d'audit expliquées ci-après.

Ces opérations peuvent nécessiter l'intervention d'une « personne habilitée» soit sur site, soit à distance, conduisant alors cette personne à ce qui est couramment appelé « prendre la main à distance ».

Les opérations de maintenance sont opérées sous le contrôle du département informatique de la CEPAL, d'IT-CE et plus généralement des filiales du Groupe en charge des systèmes.

En aucun cas, ces opérations, quel que soit leur mode opératoire, ne justifient le fait pour l'utilisateur de communiquer son identification.

Il est rappelé que, dans ce cadre, la « personne habilitée» peut être amenée à prendre connaissance de l'ensemble des éléments présent sur le poste de l'utilisateur, ainsi que des données de connexion, qu'il s'agisse d'un usage professionnel ou privé.

Si, à l'occasion d'opérations de maintenance, une utilisation anormale et/ou un contenu illicite ou préjudiciable est identifié, la CEPAL en tirera toutes conséquences en termes de responsabilité et de sanctions (*cf. article 22*).

Les utilisateurs sont informés que les opérations de maintenance font l'objet d'une traçabilité par la CEPAL.

Article 18 : Contrôle et audit

Les opérations de contrôle et d'audit se distinguent des opérations de maintenance en ce qu'elles portent sur la régularité de l'utilisation des moyens informatiques et de communication électronique.

Elles se justifient par les obligations incombant à la CEPAL.

En effet, de par son activité, la CEPAL est soumise à une obligation générale de sécurité, en application des dispositions du Code pénal relatives à la protection des systèmes de traitement automatisés de données, et de la loi dite « Informatique et libertés ».

La CEPAL, en tant qu'employeur, dispose également, en vertu du droit du travail, d'un pouvoir de contrôler l'activité des utilisateurs et en particulier, le respect par eux de la présente charte.

L'utilisation des moyens informatiques et de communication électronique pourra faire l'objet d'une surveillance afin de détecter toute utilisation non conforme, d'optimiser cette même utilisation ou encore de mener des analyses statistiques.

La CEPAL se réserve ainsi le droit, notamment :

- de vérifier le trafic informatique entrant et sortant, ainsi que le trafic transitant sur le réseau interne ;
- de diligenter des audits pour vérifier que les consignes d'usage et les règles de sécurité et de sûreté sont appliquées sur les ressources du système d'information ;

- de contrôler l'origine licite des logiciels installés ;
- de conserver des fichiers de journalisation des traces en fonction des besoins propres de chaque système d'information ;
- de transmettre aux autorités judiciaires sur requête tout ou partie des enregistrements disponibles.

En outre, en cas d'incident, la CEPAL se réserve le droit de :
- surveiller le contenu des informations qui transitent sur son système d'information ;

- vérifier le contenu des disques durs des ressources du système d'information attribuées aux utilisateurs ;
- procéder à toutes copies utiles pour faire valoir ses droits.

Ces opérations de contrôle et d'audit relèvent des fonctions de la direction de l'Audit et du responsable de la sécurité des systèmes d'information.

En particulier, dans le cadre de leurs fonctions, ils exercent un contrôle notamment des durées de connexion et des sites les plus visités. En cas de perturbation induite par l'apparition intempestive d'alertes suite à des tentatives d'infection des systèmes à l'aide de virus informatiques, elle est habilitée à mener toutes les investigations qu'elle jugera utiles aux fins d'éradiquer lesdits virus.

Les contrôles peuvent être effectués de manière globale (contrôle sur les habilitations, contrôle sur des usages …) mais également ciblés et au niveau de chaque service.

Les utilisateurs sont informés que la CEPAL est soumise également à des contrôles externes tels que ceux diligentés par l'autorité de contrôle prudentiel.

Tout intervenant de la Direction des systèmes d'information doit impérativement respecter la confidentialité des échanges électroniques et des fichiers des utilisateurs.

Les utilisateurs sont toutefois informés que les administrateurs systèmes sont conduits, de par leurs fonctions, à avoir accès à l'ensemble des informations relatives aux utilisateurs (messages, connexions à internet, etc.), y compris à celles qui sont enregistrées sur le disque dur de leur poste de travail.

Néanmoins, ces administrateurs systèmes sont tenus au secret professionnel et ne peuvent utiliser leurs droits d'administrateurs qu'à des fins strictement professionnelles.

En cas de faisceau d'indices laissant supposer qu'un utilisateur met en cause les intérêts et la sécurité de la CEPAL, en ne respectant pas les règles instituées par la présente charte, la direction de l'Organisation et des Systèmes d'Information, la direction de l'Audit, ou le RSSI se réserve le droit de fournir à la direction des Ressources Humaines, sur sa demande écrite et motivée, les traces individuelles des connexions incriminées sur une période n'excédant pas 5 ans.

En cas de non-respect avéré de la présente charte par un utilisateur, la Direction de l'Organisation et des Systèmes d'Information se verra dans l'obligation d'avertir le supérieur hiérarchique de l'utilisateur ou le Directeur de l'Audit pour que ceux-ci décident de la suite à donner.

Tout matériel installé illicitement sera supprimé ou désactivé par les intervenants de la Direction des systèmes d'information dès le constat de leur présence sur le poste de travail.

Des recommandations pourront être émises à l'issue d'un audit ou d'un contrôle faisant apparaître une violation de la présente charte et/ou de dispositions légales.

Article 19 : Mesures d'urgence et plan de continuité d'activité

L'utilisateur est informé qu'en cas de sinistre, d'incident majeur ou de nécessité impérative, la CEPAL peut mettre en œuvre un certain nombre de mesures exceptionnelles visant à assurer la continuité de son activité et le respect de ses engagements contractuels ou légaux.

Dans cette hypothèse, l'utilisateur pourra être amené à la demande de la CEPAL à prendre des mesures d'urgence et de sécurité spécifiques, qu'il s'engage à appliquer sans délai.

Ces mesures exceptionnelles peuvent inclure, notamment, une dégradation de service sur tout ou partie des ressources du système d'information (temps de réponse, capacité de stockage, d'accès ou de traitement de l'information, etc.), la suppression temporaire de l'accès à certaines ressources du système d'information (messagerie, connexion internet, accès applicatifs, éléments relatifs au poste de travail, etc.) ou la mise en œuvre de contraintes exceptionnelles (restriction temporaire de l'accès au site ou au système d'information, télétravail, déplacement sur des sites de secours tiers, etc.).

Article 20 : Consommations téléphoniques

Pour la bonne gestion de ces ressources :

- un système de communication ToIP est mis en place et permet d'enregistrer, pour chaque poste téléphonique fixe, des éléments relatifs aux communications (date, heure, durée, coût, numéros entrants et sortants dans le respect des recommandations édictées en la matière) ;
- pour les moyens informatiques et de communication électronique nomades (téléphone portable, BlackBerry, etc.), les mêmes informations sont disponibles via les opérateurs téléphoniques mobiles, à travers les services de suivi des consommations qu'ils proposent.

Les utilisateurs sont informés que les flux téléphoniques vers l'étranger sont contrôlés.

Les informations ainsi disponibles, qui sont principalement dédiées à l'analyse des consommations, peuvent en tout état de cause être utilisées pour démontrer toutes utilisations contrevenantes aux termes de la présente charte ou pour servir de preuve d'un fait manifestement illicite.

En dehors des cas prévus par le Règlement Intérieur (articles 11.10 et 11.11), toute initiative personnelle d'enregistrement des conversations téléphoniques est strictement interdite.

Dans un souci de préservation de la confidentialité de leurs communications et plus généralement du libre exercice de leurs fonctions, les représentants du personnel et/ou titulaires de mandats syndicaux peuvent demander des lignes non connectées au système de communication de l'entreprise.

Article 21 : Règles de conservation et de sauvegarde

Les utilisateurs sont informés que la CEPAL est soumise à des obligations particulières en matière d'archivage et notamment à la réglementation bancaire.

L'utilisateur est dans l'obligation, de respecter les consignes éventuelles de conservation et d'archivage mises en place par la CEPAL.

Les traces détaillées d'activité sont conservées pendant les durées légales ou conventionnelles, à l'issue desquelles elles sont détruites.

Ces traces valent preuve de l'utilisation des moyens informatiques et de communication électronique.

Ces traces peuvent faire l'objet d'un traitement statistique.

Ces traces peuvent être fournies 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 «données à caractère personnel».

Les sauvegardes réalisées par la CEPAL ne concernent pas les éléments du répertoire « PRIVE », qui sont donc conservés sous la seule et entière responsabilité de l'utilisateur.

Article 22 : Responsabilité et sanctions

L'utilisateur est responsable :

- dans le cadre de son activité professionnelle, de l'utilisation des moyens informatiques et de communication électronique en conformité avec la présente charte ;
- dans la sphère de sa vie privée résiduelle, seul, à l'exclusion donc de toute responsabilité de la CEPAL, de tout usage à caractère non professionnel.

Toute utilisation non conforme aux conditions et limites définies par cette charte est constitutive d'une faute.

En conséquence, le non-respect de la réglementation applicable expose l'utilisateur en cause à des sanctions disciplinaires, prévues par l'article 9 du règlement intérieur, et/ou à des poursuites judiciaires.

Ces sanctions peuvent également consister, notamment, dans le contrôle renforcé, la suspension, le blocage, le retrait et même la suppression pure et simple de son droit d'utiliser tout ou partie de ces moyens. Il peut, le cas échéant, être également exclu des espaces collaboratifs de travail.

La CEPAL, pour sa part, déclare mettre en œuvre, par le biais notamment de la présente charte, tous les efforts nécessaires à un bon usage des moyens informatiques et de communication électronique et n'assumer aucune responsabilité au titre des agissements fautifs ou délictueux des utilisateurs auxquels elle fournit un droit d'accès.

Article 23 : Dérogation

Toute demande de dérogation aux termes de la présente charte doit être présentée, par écrit, au Directeur des Ressources Humaines qui en informera le comité interne de sécurité, et qui se réservera le droit de l'accepter ou de la refuser.

LEXIQUE

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

- « **moyens de communication électronique** » : moyens recouvrant internet et les télécommunications (équipement sans fil, carte de communication sans fil, etc.).

- « **moyens informatiques** » : moyens recouvrant tout matériel informatique (câblage, périphérique, disquette, CD-Rom, clé USB, etc.).

- « **matériel nomade** » : moyens informatiques et de communication électronique portables, pouvant en conséquence être utilisés à l'extérieur des locaux de la CEPAL.

- « **donnée à caractère personnel** » : toute information relative à une personne physique identifiée ou identifiable (personne concernée), directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.

- « **back up** » : Recopie d'un serveur de production sur un autre site, de manière qu'en cas de défaillance du serveur de production, la copie puisse être activée et servir de nouveau serveur de production.

- « **code malveillant** » : logiciel développé dans le but de nuire à un système informatique (virus, vers, chevaux de Troie, keylogger, etc.).

- « **webmail** » : service de messagerie accessible sur internet, qui permet donc l'émission, la consultation et la manipulation de courriers électroniques.