CODE DE DÉONTOLOGIE PROFESSIONNELLE DU GROUPE **MACSF**

« La vocation du groupe MACSF est d'assurer des services et des prestations de la plus haute qualité aux professionnels du monde de la santé. A cet effet, nous veillons à ce que toutes nos activités soient conduites conformément à des références élevées d'intégrité, de confidentialité, de respect et de professionnalisme.

MACSF s'engage dans une politique de tolérance zéro face à la corruption pour toutes les activités et les entités du groupe. Cette valeur commune à tous les collaborateurs s'applique au quotidien dans nos décisions et actions. Le code de déontologie professionnelle constitue le document de référence que chaque collaborateur se doit de respecter.

Nous invitons chacun d'entre vous à prendre ou à reprendre connaissance de ce code de déontologie et à veiller au respect des principes édictés. »

Stéphane DESSIRIER, Directeur Général.

SOMMAIRE

I – Préambule

La MACSF est attachée à des valeurs sur lesquelles se fonde l'adhésion de l'ensemble de ses collaborateurs.

Sa vocation est d'assurer dans les meilleures conditions, des services et prestations de la plus haute qualité aux professionnels du monde de la santé.

Pour garantir cette mission et conforter en permanence sa réputation et son image, le groupe veille à ce que ses activités soient conduites conformément à des références élevées d'indépendance, d'intégrité, de confidentialité, de discrétion, de professionnalisme, et dans le respect du droit des personnes.

Ces valeurs ont pour finalité de répondre pleinement à la confiance que placent dans la MACSF ses assurés et tous ses partenaires.

Les règles énoncées ci-après donnent à chaque collaborateur des éléments de référence dans la conduite de ses propres activités professionnelles.

Le présent code intègre :

- la charte d'éthique professionnelle de la MACSF,
- la charte d'utilisation des ressources informatiques de la MACSF.

Il est établi conformément aux dispositions du règlement intérieur en vigueur au sein de la MACSF.

Le code de déontologie vaut code de conduite.

Un exemplaire du code est remis à chaque membre du personnel qui est invité à prendre connaissance de manière attentive des règles énoncées et à les respecter.

Des normes déontologiques complémentaires s'appliquent par ailleurs à certaines catégories de personnel en fonction de leurs responsabilités spécifiques.

II – Charte d'éthique professionnelle de la MACSF

Respect des lois et règlements / Loyauté / Respect des personnes

Chaque collaborateur est tenu au respect des dispositions législatives, réglementaires et administratives applicables dans l'exercice de son activité professionnelle, ainsi que de toutes les instructions, notes et politiques internes communiquées.

Il ne peut, quel que soit son niveau de responsabilité, outrepasser ses pouvoirs d'habilitation et d'engagement, sauf autorisation hiérarchique appropriée.

Dans son travail, le collaborateur se comporte avec honnêteté, dignité et intégrité, tant vis-à-vis de ses collègues que des prospects, assurés et sociétaires et dans le cadre de tout type de relations.

La sécurité, la santé et l'intégrité physique et morale des personnes sont une préoccupation essentielle de tous les dirigeants et collaborateurs du groupe.

Ensemble, tous sont garants du respect de la dignité et de la vie privée, conformément aux lois en vigueur, ainsi que de l'épanouissement de chacun dans la vie professionnelle, en privilégiant, dans le respect, le cas échéant, des dispositions détaillées dans le Règlement intérieur :

- les relations de confiance entre collègues, ainsi qu'entre responsables hiérarchiques et collaborateurs
- la courtoisie et le respect mutuel,
- le refus de toute forme de discrimination ou harcèlement, comme la violence physique, verbale ou morale,
- la prévention des risques psychosociaux en appliquant les dispositions de l'accord collectif en vigueur dans l'entreprise,
- le respect de l'égalité professionnelle entre les collaborateurs femmes et hommes, pendant tout le temps de leur activité au sein de l'entreprise, par l'application des principes suivants :

    - interdiction de toute discrimination en matière d'embauche,
    - absence de différenciation en matière de rémunération et de déroulement de carrière,
    - information de tous les collaborateurs, candidats à l'embauche et représentants du personnel, du dispositif de prévention du harcèlement sexuel dans l'entreprise détaillé dans le règlement intérieur.

Confidentialité de l'information / Obligation de discrétion

La protection par la MACSF de ses données propres et de celles qui lui sont confiées constitue un engagement majeur sur lequel repose la confiance de ses assurés.

Chaque collaborateur s'engage ainsi à respecter la confidentialité des informations dont il a connaissance dans le cadre de son activité professionnelle, qu'elle provienne de l'entreprise ou de tout tiers.

Cette obligation de confidentialité s'impose aussi bien à l'intérieur qu'à l'extérieur de l'entreprise et continue à s'imposer aux collaborateurs ayant quitté l'entreprise.

Ainsi :

Tous les membres du personnel de la MACSF sont tenus au respect absolu de la confidentialité des informations non publiques détenues, reçues ou traitées, qui leur sont confiées par la MACSF ou par les assurés (informations personnelles sociétaires, médicales, bancaires, données collaborateurs…) et, le cas échéant, au respect du secret médical.

Ils ne doivent diffuser ni divulguer de telles informations à aucune personne, à l'exception :

- des collaborateurs MACSF qui ont besoin de connaître ces informations dans le cadre de leurs responsabilités,
- de certaines personnes extérieures au groupe, dans le cadre d'un mandat spécifique ou d'une mission émanant de la MACSF (avocats, experts comptables, médecins experts, auditeurs, consultants…),
- des autorités publiques et de contrôle compétentes, pour les collaborateurs qui en ont la charge,
- lorsque cette divulgation est autorisée par la loi.

Chaque collaborateur prend les dispositions nécessaires pour protéger la confidentialité des informations dont il dispose en raison de son activité professionnelle.

Les informations confidentielles incluent également les informations non publiques pouvant être utilisées par les concurrents ou dommageables au groupe MACSF ou à ses assurés si elles étaient diffusées.

Sont également concernés la propriété intellectuelle ; par exemple des informations sur la conception des produits, les chiffres de l'activité, les plans marketing et commerciaux y compris les études clients, les informations sur les salaires, les données comptables, financières et celles concernant les placements, toutes les bases de données et tous les rapports non publiés de quelque nature que ce soit et quelle que soit la forme qu'elles peuvent prendre.

Communication d'informations privilégiées

Tous les membres du personnel :

s'abstiennent impérativement d'utiliser à des fins personnelles, directes ou indirectes ou de communiquer à des tiers, les informations sensibles dont ils ont connaissance,

doivent s'abstenir, sauf accord ou habilitation spécifique de la Direction Générale, de prendre contact avec les médias, afin de communiquer des informations confidentielles ou sensibles, concernant, tant les activités du groupe que les relations avec les assurés,

sont tenus à une obligation de discrétion au sein des diverses entités du groupe.

Ils s'interdisent par là même de divulguer les informations sensibles qu'ils détiennent à des collègues et/ou des entités dont les fonctions ne nécessitent pas cette communication.

Les interdictions citées ci-dessus prennent fin dès lors que les informations ont été diffusées officiellement au sein du groupe ou portées à la connaissance du public.

Intégrité / Prévention et règlement des conflits d'intérêts

Chaque collaborateur du groupe MACSF est tenu de prendre toutes les mesures nécessaires, notamment avec l'appui de sa hiérarchie, pour éviter de se retrouver en situation de conflit d'intérêt.

Ses décisions, fondées sur un principe d'intégrité, ne doivent pas être influencées ou altérées par des considérations d'ordre personnel.

Toute fonction de salarié ou de mandataire social, détenue dans une société concurrente ou pouvant interférer avec les intérêts du groupe est incompatible avec l'exercice d'une activité professionnelle à la MACSF, sauf autorisation expresse de la Direction Générale.

Les situations de ce type doivent être portées à la connaissance de la Direction des Ressources Humaines qui se réserve la possibilité de demander au collaborateur de donner sa démission au titre de ses activités extérieures (contrat de travail, mandat) en cas de situation de conflit d'intérêt.

Acceptation de cadeaux et autres avantages reçus de tiers à l'entreprise

L'acceptation de cadeaux et autres avantages est interdite pour tous les collaborateurs de la MACSF, dès lors que les intérêts du groupe en sont affectés ou si l'indépendance professionnelle du salarié risque de s'en trouver compromise.

Les cadeaux, dons et repas offerts par des partenaires peuvent cependant être considérés, dans des limites prédéfinies, conformes aux usages de la profession et constituer un moyen légitime de nouer et d'entretenir une relation d'affaires.

Dans ce cadre, le collaborateur ne doit ni demander ni accepter aucun présent ou avantage dépassant les niveaux notoirement admis, notamment en termes de valeur, laquelle doit rester faible.

L'acceptation de cadeaux et autres avantages distribués par des tiers ou partenaires du groupe MACSF, et dont la valeur est supérieure à 100 € n'est ainsi autorisée que dans les conditions non cumulatives suivantes :

- ✓ les cadeaux ou invitations à des repas d'affaires qui ne peuvent être refusés doivent être signalés au responsable hiérarchique,
- ✓ pour les invitations à des événements sans dominante professionnelle, comme un concert, une pièce de théâtre, une manifestation sportive, le collaborateur doit s'assurer que sa participation est conforme aux usages de la profession et en informer sa hiérarchie.

Dans un souci de traçabilité, chaque collaborateur établit annuellement la liste des cadeaux et avantages dont il a bénéficié pour permettre à la MACSF d'exercer tout contrôle approprié, le cas échéant.

Attribution de cadeaux et autres avantages à des tiers à l'entreprise

L'attribution de cadeaux et autres avantages à des tiers peut, dans des limites prédéfinies, être conforme aux usages de la profession et constituer un moyen légitime de nouer et d'entretenir une relation d'affaires.

Ces pratiques peuvent cependant engendrer des conflits d'intérêts latents, menacer l'indépendance de nos partenaires commerciaux et porter atteinte à la réputation de la MACSF.

En conséquence, aucune attribution de cadeaux et autres avantages à des partenaires externes au groupe MACSF :

ne doit être faite/réalisée dans l'intention d'obtenir des contreparties injustifiées,

ne doit aller à l'encontre des règles déontologiques du bénéficiaire dont le collaborateur MACSF doit s'être préalablement informé.

La transparence de ce type d'attribution est subordonnée aux conditions suivantes :

- information préalable du supérieur hiérarchique quant à l'identité du bénéficiaire et l'objet du cadeau ou de l'avantage,
- la valeur estimative ne doit pas dépasser 100 € pour les bénéficiaires, qui ne peuvent en aucun cas être des collaborateurs du groupe MACSF,
- les invitations à des repas d'affaires sont acceptées dans le cadre des grilles et procédures de remboursement de frais en vigueur dans l'entreprise.

Dans un souci de traçabilité, chaque collaborateur établit annuellement la liste des cadeaux et avantages qu'il a consenti pour permettre à la MACSF d'exercer tout contrôle approprié, le cas échéant.

Attribution de cadeaux et autres avantages reçus au sein de l'entreprise

La distribution de cadeaux ou autres avantages au sein du groupe MACSF est soumise à validation.

En effet, la Direction des Ressources Humaines doit être préalablement informée de tout dispositif concourant à ce genre de pratique, que ce soit dans le cadre d'activités courantes ou d'évènements exceptionnels. Notamment, les cadeaux, séjours ou titres de transport, les boîtes cadeaux et les chèques cadeaux distribués en dehors du Comité d'Entreprise sont considérés comme des avantages en nature.

Leur valeur est susceptible de réintégration dans le bulletin de paie du bénéficiaire, pour être soumise dans son intégralité aux cotisations sociales et à l'impôt sur le revenu.

Souscription des contrats d'assurance

Les collaborateurs MACSF bénéficient de conditions tarifaires avantageuses. De ce fait, ils doivent impérativement être propriétaires ou locataires (selon la nature du risque) des biens qu'ils assurent.

Véhicules de fonction et/ou de société

Le covoiturage à but lucratif et plus généralement tout transport monétisé, sous quelque forme que ce soit, de passagers sont formellement interdits.

Information des clients : Déontologie professionnelle / Devoir de conseil

Dans le cadre de ses fonctions, le collaborateur MACSF se doit d'avoir la meilleure connaissance possible du client afin de lui proposer une offre commerciale adaptée à son profil et ses attentes et lui communiquer toutes les informations nécessaires à l'accomplissement des opérations projetées.

Il a ainsi pour mission :

d'identifier avec rigueur le client, s'enquérir de ses besoins et, selon les cas, de sa situation personnelle, patrimoniale et financière,

de s'assurer de sa sensibilité à une prise de risque chaque fois que cela s'avère nécessaire,

d'apporter une information claire et objective en veillant à ce que la proposition effectuée réponde à la meilleure adéquation entre les besoins exprimés et la formule retenue,

de s'assurer de sa bonne compréhension des produits et services qui lui sont proposés afin de préserver sa situation financière et patrimoniale en toutes circonstances.

Lutte Anti-Blanchiment et Financement du terrorisme / Devoir de vigilance

Les organismes financiers et sociétés et mutuelles d'assurance sont soumis aux obligations relatives à la Lutte contre le blanchiment des capitaux et le financement du terrorisme (LCB- FT).

Les obligations LCB-FT s'appliquent à l'assurance vie et non vie des branches d'assurances 1 à 26. En conséquence, **toutes les entités du groupe MACSF sont concernées.**

L'Autorité de Contrôle Prudentiel et de Résolution (ACPR) a la charge de surveiller la mise en œuvre par les organismes financiers et sociétés et mutuelles d'assurances des mesures de LCB-FT, prévues par la législation en vigueur.

Dans ce cadre, le groupe MACSF applique une politique de connaissance du client fondée sur le risque et a mis en place une organisation interne et des procédures écrites ainsi qu'un système de surveillance permettant de vérifier le respect de ces procédures et tout particulièrement l'information et la formation de tous les membres du personnel concernés.

À ce titre une Norme interne présente le **socle commun** applicable au sein du groupe en matière de LCB-FT. **Ces dispositions sont complétées** par chacune des entités concernées en fonction de leur activité, de leur exposition au risque de blanchiment des capitaux et financement du terrorisme (BC-FT) et de leurs spécificités.

Chaque entité du groupe désigne une personne responsable de la mise en œuvre du dispositif d'évaluation et de gestion des risques de BC-FT et des « Correspondants et Déclarants TRACFIN ». Un dispositif centralisé d'analyse des anomalies et des déclarations des opérations à TRACFIN est mis en place et décrit dans la Norme interne précitée.

Les collaborateurs s'engagent plus particulièrement à respecter les dispositions suivantes :

s'assurer de l'identité du client,

veiller à l'enregistrement et à la mise à jour des informations et coordonnées personnelles essentielles,

veiller à la cohérence des opérations effectuées,

rendre immédiatement compte à la hiérarchie et/ou au Correspondant TRACFIN de toute opération inhabituelle ne paraissant pas avoir de justification économique ou d'objet licite,

refuser toute relation contractuelle avec un client potentiel dont on ne peut connaître l'identité, l'origine des fonds.

La transgression des règles ci-dessus est susceptible d'entraîner la responsabilité pénale du collaborateur ou de la MACSF.

Lutte contre la corruption et le trafic d'influence

Les obligations issues de la loi n°2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique dite loi « Sapin 2 » modifiée en matière de lutte contre la corruption et le trafic d'influence s'appliquent **à toutes les entités du groupe MACSF**.

L'Agence Française Anticorruption (AFA) a été créée par la loi « Sapin 2 » et contrôle le dispositif de prévention du risque de corruption mis en place par les entreprises concernées : elle peut vérifier sur pièce et/ou sur place que les entreprises satisfont à l'obligation de vigilance issue de la loi « Sapin 2 ».

Dans ce cadre, le groupe MACSF a mis en place des mesures et procédures de prévention, détection et remédiation des faits de corruption et de trafic d'influence et un dispositif de contrôle et d'évaluation interne de la mise en œuvre de ces mesures et procédures au sein de chacune des entités.

Une Norme interne présente le **socle commun** applicable au sein du groupe MACSF en matière de lutte contre la corruption et le trafic d'influence. **Ces dispositions sont complétées** par chacune des entités concernées en fonction de leur activité, de leur exposition au risque de corruption et de trafic d'influence et de leurs spécificités.

Par ailleurs, un dispositif d'alerte interne a été mis en place, complété par un dispositif de protection des lanceurs d'alerte (dispositif unique d'Alerte), tel que détaillé au chapitre IV et dans les annexes 1 et 2 au présent code de déontologie.

Les collaborateurs MACSF s'engagent plus particulièrement à respecter les dispositions suivantes :

- dispositions du présent code de déontologie, valant code de conduite annexé au règlement intérieur et notamment les règles encadrant les cadeaux et invitations,
- mesures et procédures de prévention et de détection des faits de corruption et de trafic d'influence mises en place par le groupe MACSF.

Tout collaborateur MACSF peut également procéder à un signalement, conformément au dispositif unique d'Alerte, de tout fait susceptible de constituer un délit de corruption ou de trafic d'influence.

La transgression des règles ci-dessus est susceptible d'entraîner la responsabilité pénale et/ou civile du collaborateur et/ou de la MACSF.

III. Charte d'utilisation des ressources informatiques de la MACSF

La présente charte précise les règles et précautions que tout utilisateur doit respecter, afin de garantir la sécurité des systèmes d'informations et des ressources mises en œuvre par le groupe MACSF. Elle précise également les rôles et responsabilités de chacun au sein de l'entreprise en accord avec les exigences légales, réglementaires et contractuelles en vigueur et les règles de déontologie.

Elle s'applique à toute personne, dans l'exercice de ses activités au sein du groupe MACSF et à toute personne agissant au nom et/ou pour le compte du groupe MACSF.

En cas de non-respect de cette charte, le groupe MACSF peut restreindre ou supprimer les accès de(s) l'utilisateur(s) concerné(s) aux ressources du Système d'Information. Le non-respect de la charte peut également conduire à des sanctions disciplinaires pour les collaborateurs, aux conditions prévues dans le règlement intérieur.

Le terme « utilisateur » englobe toute personne, quel que soit son statut, appelée à créer, consulter et mettre en œuvre ces ressources, de manière permanente ou occasionnelle.

Le terme « ressource » intègre :

les systèmes informatiques (locaux, distants, de bureautique, de messagerie…)

les réseaux et vecteurs de communication (téléphone, internet, télécopie…)

les matériels, logiciels, applications et processus de traitement des données

les dispositifs de sécurité (contrôle d'accès, stockage, sauvegarde…)

les procédures de création, mise à jour et d'échange d'information (disques d'échanges, transverses…)

l'information elle-même, en tant que « donnée » que le groupe MACSF utilise dans le cadre de son activité

Responsabilité des utilisateurs

Utilisation des ressources

L'utilisation inadaptée des ressources mises à disposition par le groupe MACSF, est susceptible d'engendrer des risques auxquels l'entreprise se doit d'être vigilante.

Ainsi, les ressources mises à la disposition des utilisateurs s'effectuent dans le respect :

des libertés individuelles : les utilisateurs s'interdisent de porter atteinte directement ou indirectement aux droits des personnes ainsi qu'à leur vie privée,

des règles de protection du droit d'auteur : les utilisateurs s'interdisent de copier des logiciels ou utiliser toutes œuvres telles que photographies, vidéos (…) protégées par la loi sur la propriété intellectuelle,

de la protection des données personnelles/nominatives : conformément à la Loi informatique et libertés du 6 janvier 1978 modifiée ainsi qu'à la législation applicable depuis le 25 mai 2018 découlant de l'adoption du Règlement Européen 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (« RGPD »), ainsi qu'à toute autre législation applicable ultérieurement qui pourrait les compléter et/ou les remplacer,

du devoir de réserve : les messages transmis par messagerie et/ou déposés sur des réseaux sociaux ne peuvent être exploités à d'autres fins que celles prévues par l'émetteur et porter ainsi préjudice au groupe MACSF,

de l'ordre public et des bonnes mœurs : les utilisateurs s'interdisent de manipuler des informations à caractère injurieux, diffamatoire, raciste, xénophobe, révisionniste ou pédophile, ou pouvant constituer une incitation à la haine, la violence ou la débauche, ou de prosélytisme en faveur de religions ou sectes.

L'utilisation des ressources de la MACSF n'est possible que dans le cadre de l'activité professionnelle des utilisateurs, définie par leur fonction, et dans les limites des délégations et/ou habilitations qui leur sont accordées.

Un usage personnel ponctuel et raisonnable des ressources mises à disposition par l'entreprise, justifié par les besoins de la vie personnelle et familiale, est admis dès lors qu'il ne porte pas préjudice à l'activité professionnelle et qu'il n'est pas susceptible d'affecter le bon fonctionnement des ressources informatiques ou de porter atteinte au patrimoine de l'entreprise. L'utilisation pour motif personnel du téléphone mobile à l'étranger (appels, messages, données cellulaires 3G/4G/5G) est interdite sauf en cas d'urgence.

Le groupe MACSF respecte le caractère confidentiel de cette utilisation personnelle dès lors que cette dernière est signalée comme telle.

Tout message électronique émis ou reçu étant présumé professionnel, les utilisateurs souhaitant préserver le caractère personnel de leur message sont invités à faire figurer dans leur objet la mention « personnel ». Les fichiers privés seront stockés sur l'environnement de travail dans un dossier identifié « personnel », exclusivement réservé à cet usage.

Accès aux ressources

L'accès aux ressources du système d'information est soumis à l'usage d'authentifiants (mots de passe, générateur de codes à usage unique…), **strictement personnels**. L'utilisation de ces mots de passe engage la responsabilité du titulaire. L'utilisateur s'engage à choisir des mots de passe sûrs (mot de passe différent de l'utilisateur, de la date de naissance, des prénoms des enfants…) et à les garder secrets à l'égard de toute personne.

> L'utilisateur s'interdit d'accéder aux ressources en utilisant l'habilitation d'un tiers, sans son consentement ou de contourner les restrictions d'utilisation mise en place.

Toute perte d'un moyen d'authentification ou toute anomalie relative à l'utilisation de son identifiant doit être immédiatement signalée par l'utilisateur au Responsable Sécurité des Systèmes d'informations.

L'utilisateur s'engage à verrouiller ou fermer toutes les sessions en cours sur son environnement de travail en cas d'absence, même momentanée.

Protection de l'information / Protection des données

La protection de l'information vise avant tout à assurer sa disponibilité, son intégrité et sa confidentialité.

> L'utilisateur doit respecter la confidentialité des informations auxquelles il a accès dans le cadre de sa mission.

Les dispositions de l'article 121 de la loi « informatique et libertés » obligent à prendre toutes précautions utiles afin de préserver la sécurité des informations nominatives et d'empêcher en particulier qu'elles ne soient déformées ou endommagées ou que des tiers non autorisés y aient accès.

> L'utilisateur amené dans le cadre de ses fonctions à manipuler des fichiers ou à intervenir sur les ressources du groupe MACSF s'abstient de prendre connaissance de leur contenu en dehors du strict exercice de sa mission.
>
> L'utilisateur s'interdit de perturber le bon fonctionnement du système d'Information par des manipulations anormales des ressources mises à sa disposition, ou en contournant les dispositifs de sécurité mis en place.

Il veille à ce que les données, fichiers qu'il exploite soient régulièrement sauvegardés (exemplaire unique d'un fichier sur disque local de l'ordinateur par exemple).

Protection des équipements

En protégeant les équipements qui lui sont confiés et en adoptant une attitude responsable, l'utilisateur garantit la sécurité des informations placées sous sa responsabilité.

L'utilisateur est responsable de la protection des équipements mis à sa disposition. À ce titre, il veille particulièrement à :

utiliser les moyens disponibles pour garantir la protection des équipements transportables (ordinateurs portables, téléphones portables…) et de leurs accessoires : rangement dans un tiroir ou une armoire fermant à clé…

signaler sans délai aux équipes informatiques et à sa hiérarchie toute perte ou vol d'un équipement mis à sa disposition. La perte d'équipement mobile doit être déclarée particulièrement rapidement afin de bloquer l'équipement et procéder à son effacement à distance.

Utilisateurs « nomades »

L'accès distant au Système d'Information de la MACSF depuis un équipement professionnel ou personnel du collaborateur doit respecter les règles de sécurité de la MACSF.

Dans le cas de la perte ou du vol de son équipement professionnel ou personnel utilisé pour accéder au Système d'Information, l'utilisateur doit prévenir sans délai les équipes informatiques du groupe MACSF.

Lors de déplacements à l'extérieur des locaux du groupe MACSF (réunions ou conférences, formations intra ou extra professionnelles, lieux publics, moyens de transports…), la protection des informations doit être assurée. Les supports informatiques, les contenants, supports amovibles, ordinateurs portables, téléphones mobiles ne doivent pas être laissés sans surveillance ou en évidence.

Les informations sensibles ou stratégiques de l'entreprise ne doivent pas être consultées lorsque l'environnement ne permet pas de garantir que des personnes non autorisées ne peuvent s'approprier ces informations.

Contrôle de l'utilisation des ressources

L'enregistrement des accès ou tentatives d'accès aux ressources constitue une mesure de sécurité dont la finalité première est d'en garantir l'utilisation normale. Le groupe MACSF a la faculté technique d'identifier et de sanctionner les usages contraires à la loi et à ses règles internes et doit pouvoir répondre aux requêtes des autorités relatives au comportement de ses collaborateurs.

Les mesures de contrôle mises en œuvre évoluent avec le système d'information. Elles sont décrites en annexe qui sera mise à jour régulièrement et mise à disposition sur l'intranet.

Collecte des informations personnelles

Le groupe MACSF s'engage à ce que les données concernant les utilisateurs soient collectées et traitées de manière loyale, licite et transparente.

L'utilisateur est informé que les informations le concernant, traitées dans le cadre de la gestion des ressources humaines ou dans le cadre des contrôles précités, sont destinées aux responsables habilités du groupe MACSF et qu'il dispose d'un droit d'accès et de rectification dans les conditions suivantes :

> L'utilisateur dispose d'un droit d'accès aux informations nominatives le concernant, ainsi que du droit de rectification le cas échéant dans les conditions de la loi informatique, fichiers et libertés du 6 janvier 1978 modifiée ainsi que du RGPD.

Ce droit d'accès et/ou de rectification s'exerce auprès des Ressources Humaines ou auprès du Délégué à la Protection des Données (DPO) du groupe MACSF de la manière suivante :

- Par email : dpo@macsf.fr
- Par courrier : MACSF - Secrétariat Général, Juridique et Conformité Groupe –
  10 cours du Triangle de l'Arche TSA 40100 92919 La Défense Cedex.

Pour plus d'informations s'agissant du traitement des données personnelles des utilisateurs, l'utilisateur peut consulter la Charte de protection des données personnelles en matière de Ressources Humaines.

La durée de conservation des traces informatiques peut résulter d'obligations légales. La durée maximum de conservation des traces informatiques est de douze mois.

Modalités d'accès aux données et aux traces informatiques des collaborateurs

Protection de l'intégrité et du bon fonctionnement des systèmes

Le bon fonctionnement des systèmes d'information et leur protection nécessitent une surveillance technique permanente afin de détecter et corriger les pannes, les virus, les attaques, les intentions malveillantes ou frauduleuses, les piratages, etc. Cette surveillance est assurée par les administrateurs informatiques de la Direction des Systèmes d'Information.

Dans le cadre de leur fonction, les administrateurs informatiques peuvent ainsi être amenés à accéder aux messages électroniques ou aux fichiers des espaces personnels à stricte fin de les débloquer ou d'éviter des démarches hostiles.

Des outils permettent également :

de détecter et de filtrer, **a priori** et automatiquement, tout type de connexion, fichier ou message non conforme ou présentant un risque pour le Système d'Information du groupe MACSF. À ce titre, des dispositifs de lutte contre les courriers électroniques non sollicités, les logiciels malveillants (virus, vers, chevaux de Troie…) et de filtrage des sites Internet sont mis en place.

d'analyser et de contrôler, **a posteriori,** les traces informatiques à des fins de surveillance du réseau et des systèmes ou d'analyse d'incidents.

Processus exceptionnel d'accès aux données et aux traces des utilisateurs

L'accès aux données telles que les fichiers, les traces d'accès aux ressources du SI ou les messages d'un utilisateur du groupe MACSF qui ne mentionnent pas le caractère personnel ne pourra être effectué qu'avec l'accord de l'intéressé ou dans l'une des conditions suivantes :

Nécessité de service sérieuse. L'intéressé en sera informé par mail avec le motif de l'intervention.
En cas de comportement contraire au règlement intérieur et au présent code de déontologie.

Dans ces deux cas, l'accès ne peut être effectué que sur demande explicite de la Direction Pilotage et Risques ou de la Direction des Ressources Humaines. L'opération est alors réalisée par un administrateur informatique sous le contrôle du Responsable de la Sécurité du Système d'Information.

IV - Dispositif d'Alerte interne / Procédures de recueil des signalements et de traitement des alertes

Chaque collaborateur MACSF doit, individuellement, s'approprier les règles éthiques et professionnelles du présent code et les faire vivre au quotidien.

Il incombe à chaque manager d'accompagner scrupuleusement cette démarche qualitative permanente, objectif supérieur du groupe.

Conformément aux dispositions de l'article 17, 2° de la loi « Sapin 2 », un *« dispositif d'alerte interne destiné à permettre le recueil des signalements émanant d'employés et relatifs à l'existence de conduites ou de situations contraire au code de conduite de la société »* a été mis en place, complété par le dispositif de signalement et de protection des lanceurs d'alerte visé par les articles 6 à 16 de cette loi.

Ainsi, tel que détaillé dans les annexes 1 et 2, tout collaborateur peut bénéficier du statut de lanceur d'Alerte s'il signale ou divulgue, sans contrepartie financière directe et de bonne foi :

- des informations portant sur un crime, un délit, une menace ou un préjudice pour l'intérêt général, une violation ou une tentative de dissimulation 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, du droit de l'Union européenne, de la loi ou du règlement,

- des faits constitutifs des infractions de corruption et/ou de trafic d'influence, contraires au présent code de déontologie.

Lorsque ces informations n'ont pas été obtenues dans le cadre des activités professionnelles, le lanceur d'alerte doit en avoir eu personnellement connaissance.

Le Secrétaire général et Directeur de la Conformité Groupe de la MACSF, qui occupe la Fonction Clé de Vérification de la Conformité, est garant des bonnes pratiques professionnelles en vigueur au sein de l'entreprise. En relation avec les différentes directions, et dans le respect du règlement intérieur,

- il coordonne le cadre déontologique général de la MACSF et le processus de remontée des informations, la centralisation et le traitement des Alertes internes ou des Signalements, l'établissement d'un plan de mesures correctives, l'évaluation des résultats des actions et la clôture de l'Alerte interne ou de Signalement,
- il s'assure que le présent code de déontologie et la Procédure Groupe relative au dispositif unique d'Alerte sont bien portés à la connaissance de tous,
- il détecte les conflits d'intérêts potentiels et propose des solutions.

Tout collaborateur peut saisir directement le Secrétaire général, Directeur de la Conformité Groupe par courriel [**alerte.deontologie@macsf.fr**] ou son supérieur hiérarchique en adressant le formulaire complété figurant en Annexe 2 ainsi que le cas échéant, les documents de nature à étayer son Signalement ou son Alerte interne. Dans le cadre de sa démarche, il doit respecter la Procédure Groupe figurant en Annexe 1.

La MACSF est garante de la confidentialité de l'identité de tout Auteur d'une Alerte interne ou d'un Signalement (lanceur d'alerte), afin que celui-ci ne supporte aucun préjudice du fait de sa démarche.

La MACSF est garante de la confidentialité de l'identité des personnes identifiées et mises en cause en cas d'Alerte interne ou de Signalement et des informations recueillies par le ou les destinataires de l'Alerte interne ou du Signalement.

Le droit d'accès et de rectification est ouvert au bénéfice des personnes identifiées et mises en cause sans qu'il soit possible d'obtenir l'identité de l'émetteur de l'Alerte interne ou du Signalement.

Procédure de traitement de l'Alerte interne ou du Signalement.

Chaque Alerte interne ou Signalement adressé(e) à l'adresse **alerte.deontologie@macsf.fr** fait l'objet d'une instruction rigoureuse et documentée notamment par le Comité de déontologie.

Le Comité de déontologie est composé :

- de la Directrice des Ressources Humaines ,
- du Directeur Pilotage et Risques et Fonction Clé de Gestion des Risques,
- du Directeur de l'Audit interne groupe et Fonction Clé Audit interne,
- du Secrétaire général, Directeur de la Conformité Groupe et Fonction Clé de Vérification de la Conformité.

L'émetteur de l'Alerte interne ou du Signalement est informé de la réception de celle-ci ou de celui-ci ainsi que du délai nécessaire à l'examen de sa recevabilité et des modalités suivant lesquelles il est informé des suites données à son Alerte interne ou son Signalement ainsi que de la clôture de la procédure conformément aux dispositions de l'Annexe 1.

Les propositions émises recouvrent :

- l'appréciation du manquement en question en termes d'impact interne et/ou externe
- les mesures correctrices immédiates préconisées.

La MACSF est garante de la confidentialité du traitement de l'Alerte interne ou du Signalement.

Les données relatives à une Alerte interne ou à un Signalement considéré(e), comme n'entrant pas dans le champ du dispositif, sont détruites ou anonymisées sans délai.

Lorsque l'Alerte interne ou le Signalement n'est pas suivi(e) d'une procédure disciplinaire ou judiciaire, les données relatives à cette Alerte interne ou ce Signalement sont détruites ou anonymisées dans un délai de deux mois à compter de la clôture des opérations de vérification.

Lorsqu'une procédure disciplinaire ou des poursuites judiciaires sont engagées à l'encontre de la personne mise en cause ou de l'Auteur d'une Alerte interne abusive ou d'un Signalement abusif, les données relatives à l'Alerte interne ou au Signalement sont conservées jusqu'au terme de la procédure ou de la prescription des recours à l'encontre de la décision.

Les données faisant l'objet de mesures d'archivage sont conservées, dans le cadre d'un système d'information distinct à accès restreint, par la ou les personnes habilitées, pour une durée n'excédant pas les délais de procédures contentieuses.

V – Conséquences du non-respect des règles

La violation des règles prévues par le présent code par un collaborateur est susceptible d'exposer le groupe lui-même :

- à des sanctions, tant au plan légal qu'administratif et règlementaire, qu'en termes de réputation et d'image,
- à des procédures disciplinaires engagées par l'Autorité de Contrôle Prudentiel et de Résolution ou tout autre autorité administrative pouvant aller jusqu'au retrait d'agrément d'exercer l'activité concernée.

Sous réserve de la protection accordée aux lanceurs d'alerte et selon les cas considérés, la nature du manquement en cause et en fonction des circonstances de fait, le non-respect du code peut également conduire la MACSF en conformité avec son règlement intérieur et aux dispositions générales du droit du travail, à prendre à l'encontre du collaborateur concerné, toutes mesures adaptées à la faute constatée et au préjudice engendré.