شركـــــة الهنـدســـــة الطــاقـيـــة
SOCIÉTÉ D'INGÉNIERIE ÉNERGÉTIQUE

POLITIQUE DE LUTTE CONTRE LA FRAUDE

Référence du document : **SIE-PF-01**

Date de dernière modification : **Mai 2022**

FICHE DE SUIVI DES MODIFICATIONS DU DOCUMENT

HISTORIQUE DES MISES A JOUR

	Version	*Intervenants*	*Date*	*Signature*
Elaborée par :	**V1**	**Cabinet de Conseil**	**2019**	
Mise à jour par :	**V2**	**SIE**	**Mai. 2022**	
Validée par :	**V2**	**Comité d'Audit et Risques**	**2022**	
Approuvée par :	**V2**	**Conseil d'Administration de la SIE**	**2023**	

Table des matières

CONTEXTE

La Société d'Ingénierie Energétique (« SIE » ou « Société ») dans le cadre de son repositionnement a revu son capital organisationnel et contractuel à travers, entre autres, la revue de (i) ses process et procédures, (ii) de ses documents contractuels types, etc.

Dans le même cadre, un nouveau business modèle a été élaboré et prévoit, en plus de ses fonds propres, la gestion des fonds de ses partenaires transférés (dans le cadre d'une maitrise d'ouvrage déléguée), des dons reçus et des fonds levés, ce qui nécessite de bien s'assurer de la sensibilisation ainsi que la gestion en interne et en externe des possibilités de fraude et de détournement de fonds.

Aussi, engagée dans un effort constant de bonne gestion de son fonctionnement et de ses activités, la SIE est tenue d'adopter des règles internes destinées à mettre en œuvre les obligations légales et contractuelles en matière de prévention et de lutte contre la fraude et de les appliquer strictement à ses collaborateurs, mais aussi dans le cadre de ses relations avec les tiers.

C'est dans ce contexte que la SIE a élaboré cette politique anti-fraude qui décrit les règles et les mesures à mettre en œuvre afin de lutter contre la fraude interne et externe. Elle vient compléter les mesures de verrouillage et de contrôle déjà mis en place par la SIE, dont notamment la charte éthique de la SIE.

Chapitre n°I. OBJET, DOMAINE D'APPLICATION ET CADRE LEGAL

1.1. Objet

La présente politique traduit l'engagement de la SIE dans le cadre de la prévention et la lutte contre la fraude. Elle a pour objectif d'édicter une démarche claire et efficace et d'instaurer les principes de conduite anti-fraude auxquels tout collaborateur de la SIE doit se conformer, ainsi que de délimiter les comportements à proscrire en vue de leur capacité à mener ou être liés à des actes de fraude.

Elle présente également la démarche en matière d'investigation et de traitement de cas révélés et avérés.

La politique représente ainsi le socle sur lequel est basée la démarche anti-fraude propre à la SIE.

La présente politique est évolutive et la SIE s'engage, à travers la Structure de Contrôle Interne (CI), dans l'amélioration continue du dispositif afin de se conformer aux exigences légales applicables à la SIE.

1.2. Activités et domaine d'application

La SIE, appelée également « Super ESCO », est une société dédiée à la réalisation de programmes et de projets d'efficacité énergétique (EE) avec élargissement de ses missions pour accompagner les ESCOS et les PME.

En tant que Super ESCO, la SIE a actuellement pour mission de contribuer à la mise en œuvre de la politique nationale d'EE et de l'exemplarité de l'Etat en matière d'EE et de favoriser la réalisation d'économie d'énergie ainsi que l'émergence d'un marché des prestations et de services énergétiques.

Également, la SIE intervient via deux principaux modes pour la réalisation des projets d'EE, soit en mode « Service » ou en mode « Service + financement », ce qui l'amène à mobiliser et gérer des financements pour accomplir ses missions et projets, d'où l'importance d'une politique pratique contre la fraude.

La présente politique s'étend, ainsi, à tous les collaborateurs de la SIE et à ses différentes partenaires (prestataires, fournisseurs, sous-traitants etc.), qui doivent s'y conformer lorsqu'ils agissent au nom ou pour le compte de la SIE.

La SIE est intolérante face à la fraude. Ainsi tous les incidents de fraude doivent être signalés et enquêtés conformément au dispositif d'investigation prévu par la présente politique.

Lorsque la SIE s'engage ou s'associe à un tiers, les collaborateurs veillent à ce que les principes relatifs à la fraude, énoncées dans la présente politique soient respectées.

La réputation de la SIE pourrait être endommagée par les actes des personnes travaillant pour le compte des tiers.

1.3. Cadre légal

L'ensemble des activités de la SIE se doit d'adhérer et de se conformer à l'ensemble de la réglementation qui lui est applicable, laquelle comprend :

- Des conventions internationales que le Maroc a ratifiées ;
- Toutes les lois ayant une portée extraterritoriale qui permettent aux autorités de ces pays, de sanctionner les actes de fraude commis par des personnes et des sociétés en dehors de leurs frontières ;
- De la réglementation nationale en vigueur.

Une veille réglementaire recensant de manière exhaustive l'ensemble des textes de loi, nationaux et internationaux, applicables à la SIE est tenue et mise à jour régulièrement par la Structure Juridique de la SIE.

Chapitre n°II. DEFINITIONS ET TYPOLOGIE

2.1. Définition de la fraude

Dans son acception la plus large, la fraude peut être définie comme l'acte de « tromper délibérément autrui pour obtenir un bénéfice illégitime ou pour contourner des obligations légales ou des règles de l'entreprise ». La fraude crée, ainsi, un préjudice financier, matériel, moral ou d'image à l'organisation ou à ses clients, partenaires ou autres interlocuteurs.

Toutes les fraudes ne correspondent pas à une infraction à la législation. Certains écarts aux règles de la Société peuvent également constituer des actes frauduleux (par exemple de fausses déclarations de frais ou l'affichage de faux résultats).

La plupart des fraudes constituent toutefois des délits pénaux au Maroc, susceptibles de poursuites judiciaires : vol, escroquerie, abus de confiance, faux et usage de faux.

2.2. Les types de fraude

Détournements d'actifs

- Détournements d'actifs financiers
- Détournement de produits ou d'actifs physiques (vols de matériels, de stocks et utilisation de biens à des fins non professionnelles)
- Détournement de données et intrusion dans les systèmes d'informations (vol de données à caractère confidentiel voire vols de propriété intellectuelle, utilisation frauduleuse des données de l'entreprise, intrusion et piratage informatique).

Démarches non éthiques vis-à-vis de relations normales d'affaires

- Usage d'une situation de conflit d'intérêts, favoritisme, népotisme ;
- Comportements non éthiques préjudiciables aux partenaires, falsification de l'information sur la qualité ou la quantité des services rendus.

Elaboration et manipulation ou communication interne et externe d'informations frauduleusement erronées

- Falsification de l'information pouvant affecter la qualité des états financiers, des déclarations fiscales ou des choix opérationnels internes (par action ou omission, dans le processus d'élaboration ou dans la communication interne et externe) ;
- Falsification de données opérationnelles pouvant affecter des choix opérationnels internes : la qualité du suivi de performance des activités voire des états financiers (par action ou omission, dans le processus d'élaboration ou dans la communication interne et externe) ;
- Falsification d'informations personnelles (par exemple faux curriculum vitae à l'embauche) ;
- Dissimulation de pertes.

Corruption

- Acceptation de pots de vin
- Conflit d'intéret
- Trafic d'influence
- Etc

2.2.1. Détournement d'actifs

Il s'agit de détourner intentionnellement certains actifs de la SIE vers le patrimoine propre d'un tiers, sans contrepartie pour la SIE et dans le but de retirer un profit illégitime.
Le détournement d'actifs peut se faire sous de très nombreuses modalités (espèces, facturation, paie, notes de frais, chèque, cartes de paiements, virements, assurances…).

Le détournement d'actifs peut être réalisé par un collaborateur de la SIE (fraude interne) ou par un tiers externe à la SIE (fraude externe). Un détournement d'actif interne s'accompagne souvent d'enregistrements comptables ou de documents falsifiés ou trompeurs, destinés à dissimuler la disparition de certains actifs ou le fait qu'ils ont été donnés en garantie sans autorisation appropriée.

2.2.2. Démarches non éthiques vis-à-vis de relations normales d'affaires

Il s'agit de l'usage (i) d'une situation de conflit d'intérêt (favoritisme, népotisme, etc.) ou d'un (ii) comportement non éthique préjudiciable aux partenaires (falsification de l'information sur la qualité ou la quantité des services rendus, etc.).

Un conflit d'intérêts naît d'une situation dans laquelle un collaborateur a un intérêt personnel de nature à influer ou paraître influer sur l'exercice impartial et objectif de ses fonctions officielles. Par intérêt personnel, on entend notamment tout avantage pour lui-même ou elle-même ou en faveur de sa famille, de proches, d'amis ou de personnes ou organisations avec lesquelles il ou elle a ou a eu des relations d'affaires ou politiques.

En cas de conflit d'intérêts potentiel ou réel, les collaborateurs sont tenus d'en informer immédiatement leur supérieur hiérarchique et de se conformer à la procédure interne mise en place par la Société pour la Gestion du conflit d'intérêts.

2.2.3. Elaboration et manipulation ou Communication d'informations frauduleuses

Il s'agit de la déclaration d'informations erronées de manière volontaire, qu'elles soient d'ordre financier ou non à travers :

- La manipulation intentionnelle des comptes de la Société dans le but d'en donner une image plus flatteuse par exemple ;
- La falsification de données non financières – telles que les performances d'une activité par exemple - pouvant affecter les choix et décisions opérationnels ou stratégiques de la Société.

2.2.4. Corruption

La corruption est tout offre, promesse, don, acceptation ou une sollicitation d'un avantage indu de toute valeur (financière ou non financière), directement ou indirectement, indépendamment du ou des lieux, en violation des lois applicables, pour inciter ou récompenser une personne à agir ou à ne pas agir dans le cadre de ses fonctions.

Il est interdit à tout collaborateur de la SIE de solliciter ou d'accepter d'un partenaire, d'un fournisseur / un prestataire de service ou de toute relation professionnelle externe, toute forme de corruption dans l'exercice de ses fonctions ou une faveur d'une personne entretenant avec eux une relation d'affinité.

La corruption peut être soit, active par le fait de proposer ou d'accorder des avantages quelconques à toute personne pour qu'elle accomplisse une action ou s'en abstienne dans le cadre de ses fonctions, soit passive par le fait de recevoir des avantages quelconques pour accomplir une action ou s'en abstenir dans le cadre de ses fonctions.

Un fait de corruption existe même :

- Si celui qui propose l'avantage agit au travers d'un tiers (un intermédiaire, un agent commercial, un sous-traitant, un fournisseur, un partenaire, etc.) ;
- Si celui qui reçoit l'avantage n'en est pas le bénéficiaire final (le bénéficiaire peut être un parent, un
- tiers, etc.) ;
- Si l'action frauduleuse et l'octroi de l'avantage indu n'ont pas lieu simultanément (l'avantage indu peut être anticipé, ou accordé plus tard) ;
- Si l'avantage indu prend des formes autres que la remise d'argent (il peut s'agir d'objets matériels, de services à rendre, d'un bénéfice de réputation, etc.).

Les typologies d'actes de corruption incluent notamment le conflit d'intérêts, mais aussi le trafic d'influence qui désigne toute situation où une personne sollicite ou agrée des offres ou promesses, sollicite ou reçoit des dons, présents ou autres avantages, afin qu'elle use de son influence pour amener un tiers à prendre une décision favorable.

Chapitre n°III. GOUVERNANCE DU DISPOSITIF ET MESURES DE LUTTE CONTRE LA FRAUDE

3.1. Risques de fraude dans les activités de la Société

Tout collaborateur, dans le cadre de l'exercice de ses fonctions, peut être potentiellement exposé à une situation à risque de fraude. Pour pouvoir les prévenir et y pallier, il est nécessaire d'être capable de les identifier et les remonter, le cas échéant. A titre indicatif, quelques types de risques auxquels les collaborateurs peuvent éventuellement être confrontés :

- Chercher à favoriser l'obtention d'un contrat ou d'un marché ;
- Chercher à se trouver dans une situation privilégiée (règles favorables de préqualification, critères d'attribution, mécanismes contractuels) ;
- Chercher à obtenir des décisions favorables (extensions de délais, travaux supplémentaires, validations de quantités, avenants, réclamations, réception litigieuse, etc.).

Toutes les situations à risques ne pouvant être traitées exhaustivement, les collaborateurs doivent adresser toute question sur l'application ou l'interprétation de la politique à leurs supérieurs hiérarchiques ou aux référents désignés par la Société.

La SIE mettra en place une cartographie des risques de fraude, afin de pouvoir :

- Répondre aux exigences d'évaluation des risques ;
- Faire une revue exhaustive des différentes typologies de risques de fraude ;
- Calculer les risques objectifs et les risques opérationnels bruts et nets/résiduels ;
- Evaluer l'efficacité des dispositifs de prévention et de lutte contre la fraude existants.

3.2. Politique formalisée dédiée

Le dispositif de lutte contre la fraude et les règles de bonne conduite s'inscrivent dans le cadre de la présente politique. L'ensemble des principes décrits dans la présente politique se doivent d'être respectées.

Toute dérogation à la présente politique est transmise à la Structure Contrôle Interne et à la Direction Générale de la SIE.

La mise en œuvre de cette politique, à travers la mobilisation du personnel, les mesures de prévention et de lutte contre la fraude, est de la responsabilité première de la Direction Générale.

3.3. Règles de conduite

La SIE adhère au principe de « tolérance zéro » en matière de fraude sur l'ensemble de ses activités et pour l'ensemble de ses collaborateurs.

Aucun collaborateur ne doit donc accorder directement ou indirectement à un tiers, ni recevoir des avantages indus, de quelque nature qu'ils soient et par quelque moyen que ce soit, dans le but d'obtenir ou de maintenir une transaction ou un traitement de faveur.

Les collaborateurs sont invités à signaler les suspicions de fraude, dans les conditions de confidentialité et de sûreté prévues par le référentiel des dispositifs d'alerte mis en place par la Société. Ces conditions prévoient en particulier la protection des utilisateurs du dispositif.

Tous les collaborateurs sont tenus de se familiariser avec cette politique, et de respecter ses principes.

3.4. Comités permettant de reporter au Conseil d'Administration et à la Direction Générale

3.2.1 Comité d'audit et risques

Le comité d'audit et risques de la SIE, émanant du Conseil d'Administration, adresse la lutte contre la fraude dans son ordre du jour. Le fonctionnement de ce Comité est détaillé au niveau de sa charte qui est formalisée et approuvée par le Conseil d'Administration de la SIE, qui décrit précisément la constitution de ce Comité ainsi que ses rôles et responsabilités.

3.2.2 Comité de Direction

Le Comité de Direction « CODIR » est un comité institué pour permettre à la Direction Générale d'assurer sa responsabilité. Il prévoit dans son ordre du jour d'adresser la conformité dont notamment la lutte contre la fraude.

Le comité se réunit mensuellement. Il est présidé par le Directeur Général de la SIE, et placé sous la responsabilité du Responsable Contrôle Interne.

3.5. Reporting Périodique

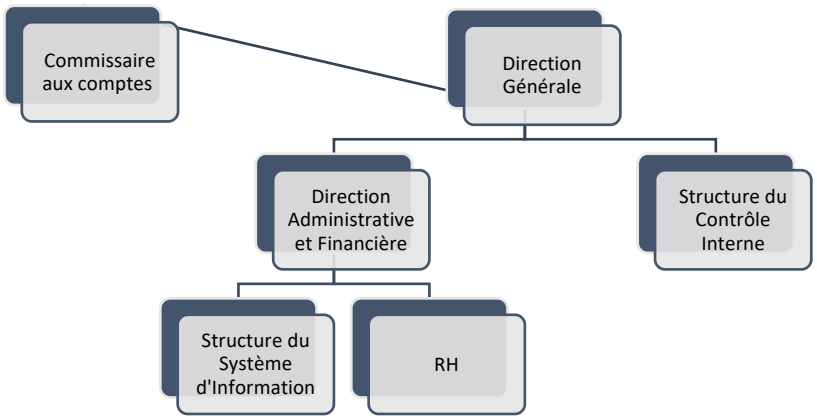
Un système de remontée périodique d'informations est mis en place par la Structure Contrôle Interne, permettant le partage des informations nécessaires au sein de la Société dont principalement :

- Etat d'avancement de la conception et du déploiement de la politique de lutte contre la fraude ;
- Résultats de contrôle et les mesures de vérification mises en œuvre à titre préventif et anticipatif ;
- Cartographie des risques de fraude qui sera mise en place ;
- Rapport des missions d'audit couvrant le dispositif de lutte contre la fraude, qui peuvent être diligentées ;
- Rapport des missions d'enquête suite à la suspicion de cas de fraude.

Une synthèse est présentée périodiquement au management et au Comité d'audit et risques.

3.6. Organisation du dispositif de lutte contre la fraude

Les principaux acteurs impliqués dans la lutte contre la fraude au niveau de l'organisation de la SIE, participent à la fois individuellement et collectivement à la mise en place et au déroulement du dispositif de lutte contre la fraude :



3.6.1. Rôles

3.6.1.1. Rôle de la Direction Générale

La Direction Générale joue un rôle actif dans la diffusion d'une culture anti-fraude. Elle assure l'engagement de la SIE dans la lutte contre la fraude.

3.6.1.2. Rôle du contrôle interne

La structure Contrôle Interne est en charge de la réalisation des investigations à la demande de la Direction Générale lorsque cela est jugé nécessaire. L'objectif est d'évaluer si la fraude s'est effectivement produite et de retracer les faits et d'établir les responsabilités (acteurs impliqués, impact financier estimé, etc.)

3.6.1.3. Rôle du Commissaire aux comptes (CAC)

Le CAC dans le cadre de son mandat d'audit prend en compte le risque de fraude dans ses missions d'audit. Les audits menés doivent notamment permettre de s'assurer que le dispositif de prévention et de détection de la fraude est conforme aux exigences de la SIE, qu'il est efficacement mis en œuvre et à jour.

3.6.1.4. Rôle de la Direction Administration & Finance (DAF)

La Direction Administration & Finance a la responsabilité de mettre en place et de mener les instructions de contrôle comptable et financier qui permettront à la SIE de s'assurer que les livres, registres et comptes ne sont pas utilisés pour masquer des faits de fraude.

Aussi, la DAF assure le rôle des Ressources Humaines, à cet effet, elle s'assure que les processus en lien avec la gestion des RH soit intègre et respectent les normes anti-fraude de la SIE. Notamment, dans le cadre du processus de recrutement, cette fonction s'assure de la vérification par tout moyen de la réputation de chaque candidat pour s'assurer de son intégrité.

3.6.1.5. Rôle de la Structure du Système Information (SI) en matière de gestion de la sécurité informatique

La structure SI est en charge de la gestion de la sécurité informatique permettant de prévenir la fraude interne et externe.

Notamment, cette structure met en place, en coordination avec les responsables hiérarchiques, un dispositif de gestion des habilitations, permettant de garantir que les accès et les habilitations, accordés aux collaborateurs, sont adéquates dans les différents systèmes d'informations selon le périmètre de leurs interventions. Ces accès sont propres à chacun des collaborateurs et ne doivent être utilisés par personne d'autre. Ils sont mis à jour au besoin, et désactivés au départ ou à la mutation du collaborateur.

La structure SI est également en charge de la gestion de la cybersécurité. Elle s'assure à ce titre de la mise en place des systèmes complets de gestion des vulnérabilités informatiques pour tous les actifs informationnels et met en œuvre des contrôles et audits réguliers pour s'assurer que les pratiques de sécurité sont conformes. Cette fonction contribue ainsi à surveiller les cyber-extorsion et d'y remédier.

Chapitre n°IV. PROGRAMME DE PREVENTION ET DE DETECTION DES RISQUES DE FRAUDE

4.1. Charte Ethique

La SIE dispose d'une Charte Ethique qui a pour objet de fixer les règles déontologiques permettant d'assurer le respect des principes d'équité, de transparence et d'intégrité nécessaires et prévenir ainsi la fraude. Elle s'applique à tous les Collaborateurs ainsi que les différentes contreparties de la SIE.

En particulier, la charte présente les grands principes en matière de gestion des conflits d'intérêt, d'éthique personnelle, de lutte contre la corruption, ainsi que les règles applicables en matière de don ou de réception de cadeaux et avantages qui peuvent constituer des actes de corruption.

La Charte Ethique est complétée par d'autres documents clés tels que le règlement intérieur ainsi que les procédures internes.

4.2. Campagne de sensibilisation

Un plan de formation anti-fraude, est établi et déployé auprès des collaborateurs de la SIE en adéquation avec les risques de fraude correspondant à chaque fonction. Des séances de sensibilisation autour des différents aspects de la prévention de la fraude sont réalisées.

4.3. Dispositif de contrôle

4.3.1. Contrôle permanent et contrôle périodique

Le dispositif de contrôle interne de la SIE – regroupant le contrôle permanent et le contrôle périodique - est indispensable à la mise en œuvre et la surveillance du dispositif de lutte contre la fraude.

Dans le cadre du plan de contrôle permanent, des contrôles sont mis en place afin de (i) s'assurer de l'application effective du dispositif de lutte contre la fraude et (ii) d'identifier les manquements liés à la mise en œuvre des dispositifs de lutte contre la fraude. Ils permettent également de détecter le manque d'efficacité et d'adéquation desdits dispositifs.

4.3.2. Processus de monitoring des procédures comptables et opérationnelles

4.3.2.1. Principes généraux des procédures comptables et opérationnelles

Les procédures comptables et opérationnelles mises en place par la Société doivent permettre de s'assurer de la fidélité, la transparence et la sincérité des opérations comptables et financières.

Chaque écriture doit être justifiée et documentée et tous les éléments relatifs à toute transaction ou opération doivent être conservés. Les opérations doivent être accompagnées de pièces justificatives suffisantes pour en comprendre la nature et l'objet. Tous les registres comptables doivent être à jour.

Les règlements effectués doivent obéir aux règles comptables marocaines.

4.3.2.2. Contrôles des procédures comptables et opérationnelles

Le contrôle des procédures permet de veiller à l'efficacité du dispositif de lutte contre la fraude et de détecter d'éventuelles infractions à partir des données comptables et financières de la SIE. Ces contrôles doivent se matérialiser par des tests sur les opérations enregistrées dans les livres, registres et comptes afin de vérifier qu'elles ne masquent pas des actes de fraude.

4.4. Dispositif de traitement des alertes et des investigations :

4.4.1. Signalement des suspicions de fraude

Tous les collaborateurs sont invités à alerter sur des faits permettant de soupçonner ou d'identifier un cas de fraude, interne ou externe.

Pour cela, les collaborateurs peuvent :

- soit aviser la ligne hiérarchique directe ou fonctionnelle (indirecte) ou saisir le Déontologue, directement, à savoir le Directeur Général ou son suppléant (nommé par la Direction Générale) ;
- soit, avoir recours au dispositif d'alerte interne en vigueur, **alerte@sie.co.ma**.

Au-delà du Déontologue, un nombre limité de collaborateurs (DAF, CI, SI) ayant pour mission de contribuer au traitement des alertes peuvent avoir accès aux informations remontées via cette adresse email. Ces collaborateurs sont formés et sensibilisés et soumis obligatoirement aux règles de confidentialité.

Afin de déposer son signalement, le lanceur d'alerte est invité à transmettre au minimum les informations suivantes :

- L'identification des personnes visées ;
- L'objet des faits signalés ;
- La description des faits faisant l'objet du signalement ;
- Des justificatifs si disponibles.

Aucun employé ne pourra être sanctionné ou faire l'objet d'une mesure discriminatoire pour avoir signalé une alerte de manière désintéressée et de bonne foi par le biais du dispositif d'alerte.

A l'inverse, toute personne qui lancerait une alerte de manière abusive (dénonciation calomnieuse, signalement effectué de mauvaise foi, etc.) s'expose à des sanctions disciplinaires et à des poursuites judiciaires.

4.4.2. Traitement des alertes & d'investigation

Chaque alerte donne lieu à une évaluation préliminaire de sa recevabilité par le Déontologue ou son suppléant au regard de la nature des faits remontés.

Le Déontologue ou son suppléant informe systématiquement le lanceur d'alerte de la conclusion de son évaluation et de ses motifs.

La personne mise en cause est également informée dans les meilleurs délais - lorsqu'il est jugé que cela ne nuira pas au bon déroulement des recherches et investigations :

Les signalements recevables peuvent être traités de 3 manières :

- Dans le cas où les allégations de fraude sont très vagues, le Déontologue ou son suppléant demande des informations complémentaires au lanceur d'alerte. Si ces informations ne peuvent pas être obtenues, le Déontologue ou son suppléant informe le lanceur d'affaire de son incapacité à faire suite au signalement ;
- Une enquête est lancée pour collecter des précisions complémentaires et identifier des preuves tangibles qui pourraient mener à renforcer ou rejeter l'allégation transmise par le lanceur d'alerte ;

- Si plusieurs éléments tangibles sont disponibles et permettent d'appuyer l'allégation, le Déontologue ou son suppléant peut alors mandater la réalisation d'une investigation pour faire toute la lumière sur les faits objets du signalement.

Il appartient au Déontologue ou son suppléant, avant chaque transmission de données à la structure Contrôle Interne, d'opérer un tri parmi ces dernières pour s'assurer que le destinataire accède aux seules données strictement nécessaires pour la réalisation de l'investigation.

Il est possible de mandater un cabinet d'audit pour réaliser les investigations nécessaires.

Dans le cadre de ces investigations, le collaborateur concerné peut être interrogé pour répondre aux interrogations de la structure Contrôle Interne, et de fournir des justifications / documents divers.

Le rapport d'investigation est transmis par la structure Contrôle Interne au Déontologue. Celui-ci inclut principalement, le contexte du dossier, les constats effectués, les preuves rassemblées ainsi que l'évaluation du préjudice subi par la Société.

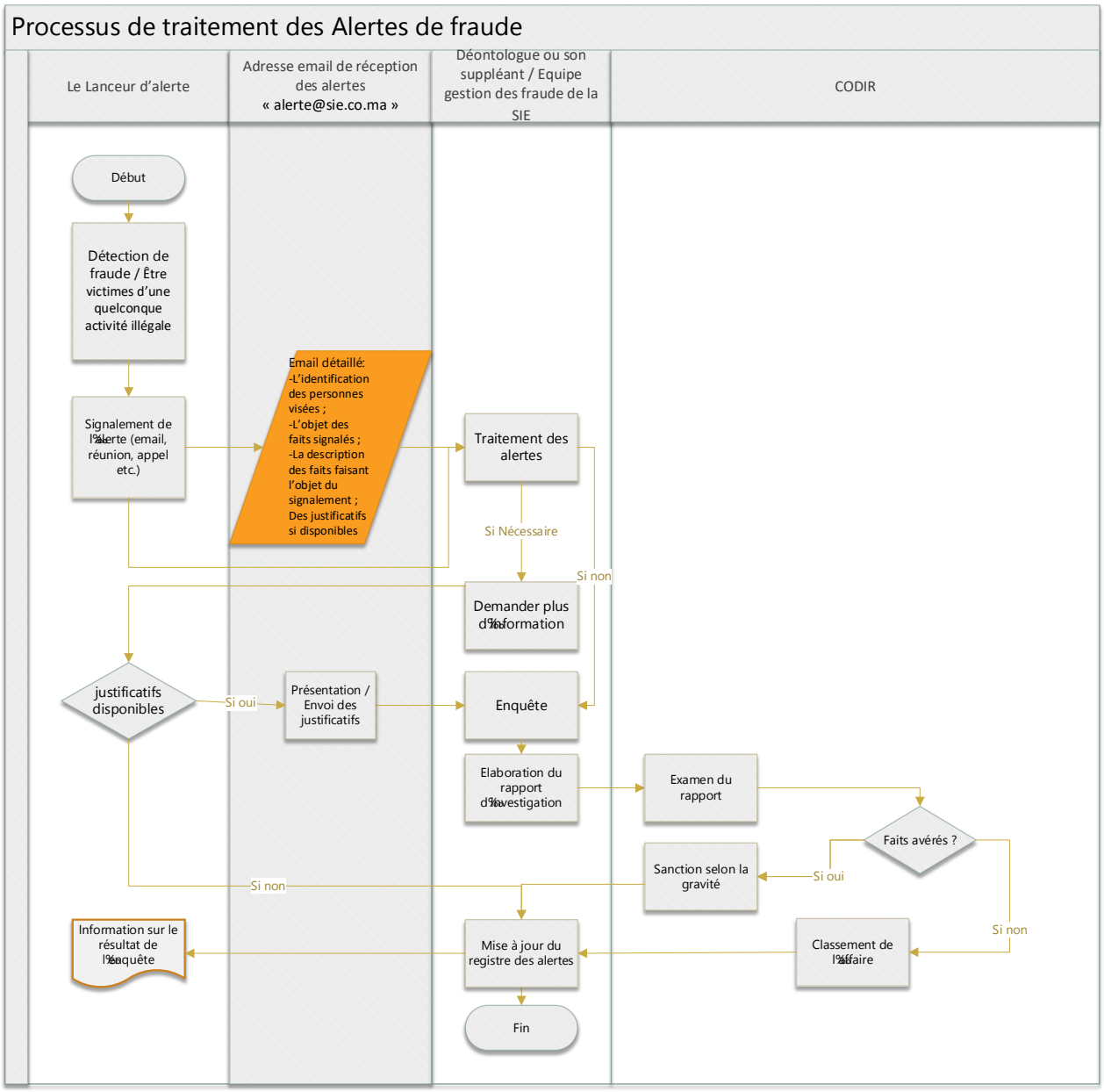
Un registre anonyme des alertes remontées est tenu et mis à jour par le Déontologue ou son suppléant.

4.4.3. Sanctions disciplinaires

Si les actes de fraude se sont avérés « Vrais », le collaborateur de la SIE s'expose aux sanctions les plus graves :

- Sanctions pénales prononcées par les tribunaux conformément à la législation en vigueur ;
- Et/ou sanction disciplinaire interne : les actes de fraude confirmés suite aux investigations seront remontés à la Direction des Ressources Humaines/ DAF et au Comité de Direction (CODIR) pour arbitrer sur les suites à donner. Les sanctions disciplinaires doivent être proportionnées au degré de l'acte et du risque.

4.5. Logigramme (Process) de traitement des alertes de fraude :



4.6. Révision de la politique

La présente politique est évolutive et devra être mise à jour par Structure Contrôle Interne, en prenant en considération des évolutions majeures survenant et la démarche d'amélioration continue du dispositif.