



Directives institutionnelles

Signalement des suspicions de fraude ou d'abus

Direction des Risques et des Audits

septembre 2025

DI | 02



Version & Date	Validée par
Version Initiale - 2019	Directoire
Version 2 – Septembre 2025	Comité Exécutif Global (GEC) et Comité Social et Economique (CSE)
Prochaine révision 2030	

Sommaire

1. Cadre Général	4
1.1. Définition du cadre	4
1.2. Responsabilité des directeurs, directrices et managers	4
2. Les modalités de signalement accessibles aux membres et personnels de HI	4
2.1 L'information de la ligne managériale	5
2.2 La possibilité d'alerter des échelons supérieurs de l'organisation	5
3. Les engagements de l'organisation.....	8
3.1 Le respect de la confidentialité.....	8
3.2 Le respect des engagements contractuels et professionnels.....	8
3.3 La sécurité.....	9
3.4 Examen des informations et traitement des cas	10
4. Les dispositifs de signalement ouverts à l'externe.....	11
4.1 Pour les bénéficiaires de nos actions	11
4.2 Pour les organismes partenaires et les fournisseurs	12
4.3 Pour les donateurs institutionnels et privés.....	12



Cette **directive institutionnelle** vient compléter : la [PI 02 Politique de protection de l'enfance](#), [PI 03 Protection des bénéficiaires contre l'exploitation, les abus et le harcèlement sexuels](#) et [PI 04 Lutte contre la fraude et la corruption](#). La **lecture préalable de cette politique est indispensable** à la compréhension des enjeux et des principes guidant la présente directive.

1. Cadre Général

1.1. Définition du cadre

Notre organisation a mis en place des mécanismes de pilotage, d'information, d'administration et de contrôle qui doivent assurer non seulement une bonne gestion de nos activités, mais aussi prévenir les agissements dont le résultat serait :

- D'affecter nos ressources, l'intégrité de notre fonctionnement et la qualité de l'aide destinée aux bénéficiaires de nos projets ;
- De porter atteinte à l'intégrité physique, psychique et à la dignité des personnes, collaborateurs et collaboratrices HI, bénéficiaires, partenaires, ou membres des communautés dans nos pays d'intervention.

1.2. Responsabilité des directeurs, directrices et managers

Ces mécanismes généraux servent de socle aux mesures spécifiques de lutte contre la fraude, la corruption et les abus. Et pour que ces mécanismes soient efficaces, les directeurs, directrices et managers ont pour responsabilité d'informer les membres et personnels de l'organisation des principes clés du contrôle interne et de notre fonctionnement. À cette fin, des mesures d'information et de formation sont prises pour sensibiliser les membres et personnels des sièges des entités du réseau fédéral et des terrains d'intervention. Pour être complète, cette information précise les modalités de signalement des suspicions et incidents. La transparence en la matière ne peut que contribuer à un climat de travail serein, qui favorise la prévention et l'utilisation des dispositifs de signalement disponibles.

2. Les modalités de signalement accessibles aux membres et personnels de HI

Les membres et le personnel de HI disposent d'un certain nombre d'options pour signaler des actes suspectés ou découverts de fraude, de corruption, d'abus et d'exploitation sexuels, de maltraitance des enfants et de tout autre abus à l'encontre d'individus, qui doivent répondre aux exigences de professionnalisme, de confidentialité et de sécurité tant pour l'individu que pour l'organisation.

2.1 L'information de la ligne managériale

- 2.1.1** La première solution est l'information de la chaîne managériale, qui demeure le canal habituel et prioritaire de signalement. Le dispositif de gestion des risques et de traitement des incidents actuellement en place s'appuie sur des référentiels, des procédures de traitement et de signalement qui privilégient une gestion ordinaire des cas par la chaîne managériale, avec l'appui des référents fonctionnels ou thématiques.
- 2.1.2** Cette voie de gestion habituelle implique une saisie du supérieur hiérarchique, accompagnée d'une information des référents spécifiques (ressources humaines, finances, etc.). En fonction du type d'incident rencontré, les responsables sur le terrain et au siège, sont sollicités pour la prise en charge du traitement de l'incident, avec l'appui des services supports concernés.
- 2.1.3** La personne qui signale une suspicion ou un incident, doit le faire dans les meilleurs délais. Il ne lui est pas demandé d'enquêter ou de constituer un dossier de preuves avant de faire le rapport. Ces tâches ne peuvent être réalisées que sur instruction explicite par des personnes désignées par la direction.
- 2.1.4** Ainsi, sur le plan formel, tous les incidents, relevant d'actes ou d'omission, involontaires ou délibérés, générant un préjudice ou un risque pour les personnes ou pour l'organisation, font l'objet d'une remontée d'information, via les supports de déclaration d'incidents disponibles, vers les niveaux de responsabilité et les services du siège les mieux à même de gérer les suspicions ou les cas avérés.

2.2 La possibilité d'alerter des échelons supérieurs de l'organisation

- 2.2.1** Toutefois, dans certaines circonstances, la personne qui suspecte ou découvre un cas de fraude, de corruption ou d'abus peut estimer difficile ou risqué de saisir l'échelon supérieur direct. Ce, pour plusieurs raisons :
- crainte que le supérieur ou la supérieure hiérarchique ne soit pas en mesure de gérer le signalement dans l'intérêt de l'association,
 - crainte que ce supérieur, ou cette supérieure, soit impliqué dans les actes faisant l'objet de la suspicion,
 - crainte d'une sanction ou de conséquences négatives plus ou moins fondées.

2.2.2 De manière concrète, la personne pourra sauter un ou plusieurs échelons hiérarchiques pour s'adresser à un responsable situé à un niveau plus élevé dans la hiérarchie, sur le terrain ou au siège. Par exemple : un employé qui estime difficile de s'adresser à son manager, alertera directement le directeur ou la directrice de programme sur le terrain, voir la direction géographique ou régionale ou à la direction des ressources humaines au siège. Bien entendu, cette logique est applicable aux différents niveaux de l'organisation, sur le terrain comme au siège, et concerne toutes les directions.

2.2.3 En plus du canal managérial et hiérarchique de remontée d'informations, notre organisation a mis en place un système centralisé (exclusivement interne), rattaché à la Direction Générale et à la Présidence Fédérale, pour recueillir les alertes professionnelles.

2.2.4 Les signalements sont reçus et suivis par une cellule composée de directeurs, directrices et de managers du département des programmes internationaux ou des entités concernées et de la direction des risques et des audits (DRA). Depuis 2020, ce système s'appuie sur une plateforme sécurisée de signalement et management de cas (EthicsPoint de NAVEX). Ce mécanisme d'alerte est accessible via la plateforme intranet de HI - HIinside ou via le site Internet de HI à tout membre ou employé de HI, au sein de l'entité fédérale, des associations du réseau, au siège ou sur le terrain.

Attention n°1 : tout responsable qui reçoit un signalement d'abus ou de fraude par la voie hiérarchique doit saisir ce signalement dans la plateforme de gestion de cas EthicsPoint. Cela s'applique également à tout employé qui reçoit un signalement de la part de membres de la communauté, de bénéficiaires de l'aide ou d'autres parties prenantes externes souhaitant alerter l'organisation par l'intermédiaire d'un employé (voir chapitre 4).

Attention n°2 : le système d'alerte professionnelle ne se substitue en aucun cas aux voies existantes de gestion des difficultés managériales et des incidents. L'alerte professionnelle est réservée au signalement des suspicions de faits suivants :

A) Abus contre les personnes

- Discrimination basée sur l'orientation sexuelle, sur la religion, sur le genre ou sur le handicap
- Racisme et discriminations basée sur l'origine ou sur la couleur de peau
- Brimades & humiliations

- Maltraitance sur enfant
- Harcèlement moral
- Harcèlement sexuel
- Abus sexuels
- Exploitation sexuelle

B) Fraude et corruption

- Fraudes en ressources humaines et conflits d'intérêts
- Fraudes logistique détournements et vols matériels
- Fraudes, extorsions et détournements sur les projets et bénéficiaires
- Vols et fraudes comptables ou financières
- Aide matérielle ou financière à des forces ou à des groupes armés
- Violation des règles de protection des données sensibles.

Un dispositif centralisé d'alerte professionnelle

La plateforme digitale EthicsPoint vise à faciliter le signalement d'incidents graves en toute confidentialité. Elle permet une plus grande réactivité, grâce à la mobilisation rapide de l'encadrement supérieur, qui peut demander la mise en œuvre de mesures internes d'enquête, de traitement et de protection.

Sur le plan pratique, à la réception de l'alerte, un premier accusé de réception automatique est produit avec un numéro de clé sécurisé permettant un suivi ultérieur par le déclarant. Seuls deux destinataires primaires automatiques (un cadre supérieur et un référent thématique) strictement identifiés dans le système et ne présentant aucun conflit d'intérêts reçoivent l'alerte et décident si des missions supplémentaires sont pertinentes ou non.

Le premier niveau de gestion des dossiers consiste à vérifier les conditions de protection du lanceur d'alerte (et des victimes individuelles/survivants dans le cadre des abus - si ne s'agit pas des mêmes personnes). Mais aussi à procéder à une première analyse pour qualifier les faits : lien avec HI, type d'allégation, gravité, détails et valeur des éléments factuels, ce qui peut conduire, selon le cas :

- soit à des contrôles par les services opérationnels et de soutien, qui conservent leurs responsabilités en matière de contrôle interne,
- soit à une enquête administrative interne, sous la responsabilité de la Direction risques et audits (DRA), visant à confirmer l'existence d'une fraude ou d'un abus et à établir les responsabilités individuelles.

Lien annexe : [Logigramme de traitement des signalements](#)

3. Les engagements de l'organisation

Ainsi, quel que soit le canal emprunté : ligne managériale, point focal/référent ou mécanisme d'alerte professionnelle, l'organisation prend les mesures d'information et de protection des membres ou employés qui sont amenés à signaler des suspicions ou des incidents, et des lanceurs d'alerte, tout au long du processus.

En effet, les utilisateurs et utilisatrices des différents dispositifs doivent être assurés des engagements de l'organisation en matière de confidentialité, de protection professionnelle et de sécurité.

3.1 Le respect de la confidentialité

HI encourage les auteurs et autrices de signalement (ou lanceurs d'alerte) à s'identifier, afin d'assurer un meilleur traitement du signalement en ouvrant la possibilité de demander des précisions complémentaires. En contrepartie, les managers destinataires de l'information et ceux chargés du traitement des incidents s'assurent que l'identité des personnes est traitée de manière confidentielle. En effet, la confidentialité est une obligation autant qu'une condition pour le traitement serein des cas signalés, avérés ou non, et pour la sécurité des personnes dans les contextes sensibles. Toutes les remontées d'information sont traitées avec la même rigueur et les mêmes conditions de sécurité. Cette confidentialité permet également de garantir la présomption d'innocence des personnes qui pourraient être mises en cause, tant que la véracité des faits n'a pas été établie par l'enquête interne, mais aussi la gestion professionnelle et sereine des cas avérés.

3.2 Le respect des engagements contractuels et professionnels

Notre organisation s'engage à ce que l'auteur ou l'autrice d'un signalement ne soit pas inquiété, à titre personnel, dans ses fonctions et dans sa carrière. En effet, aucune sanction ne peut être appliquée contre une personne qui agit de bonne foi, quels que soient les résultats de l'enquête, c'est-à-dire même si, finalement, aucune fraude ou aucun abus n'est confirmé.

A l'inverse, les personnes qui, en l'absence de toute suspicion légitime, utilisent abusivement ce mécanisme dans le seul but de nuire, pour dénoncer ou faire courir des rumeurs malveillantes, peuvent être sanctionnées.

3.3 La sécurité

Les managers en charge de la gestion des cas prendront toutes les mesures nécessaires relatives à la sécurité personnelle des auteurs et autrices de signalement et des personnes qui témoignent, pour qu'ils ne subissent aucun préjudice ni ne fassent l'objet d'aucune intimidation ou de représailles.

Voir encadré ci-après : **Protection contre les représailles.**

Protection contre les représailles

Définition : Par représailles on entend toutes mesures défavorables prises à l'encontre d'un lanceur d'alerte agissant de bonne foi, en réaction à un signalement. Les représailles peuvent concerner l'environnement de travail (climat hostile ou intimidations), les sanctions injustifiées (avertissement, suspension, licenciement), les blocages ou mises en cause de la situation ou de l'évolution professionnelle du lanceur d'alerte (freins ou refus des promotions, des augmentations salariales ou des demandes d'évolution statutaire). (Liste non exhaustive)

1. Des mesures de protection

Corolaire de l'obligation de signaler tout soupçon d'activité non- éthique, illicite, frauduleuse ou abusive, HI s'engage à protéger contre les représailles tout employé qui s'engage dans une démarche d'alerte.

1.1 HI sensibilise ses membres et personnels aux mesures de prévention et de protection contre les représailles, par les canaux habituels d'information et de formation interne.

1.2 La confidentialité étant la première des mesures de protection, HI a mis en place un mécanisme de recueil des signalements et alertes qui prévoit :

- Un protocole de traitement confidentiel des informations et des informations contenues dans les alertes,
- La confidentialité sur les sources et l'identité des auteurs et autrices de signalements
- La protection des données recueillies sur une plateforme sécurisée accessibles aux seules personnes autorisées. La vérification systématique à la fin de l'enquête et dans les 6 mois suivants (au moins 2 fois sur la période) de la situation du lanceur d'alerte.

1.3 A ce titre, la violation des règles de confidentialité et la divulgation d'informations personnelles sensibles, peuvent faire l'objet de sanctions disciplinaires voire de poursuites légales.

2. Conséquences de la violation des dispositions anti- représailles.

2.1 Toute suspicion ou observation de représailles à l'encontre d'un lanceur ou d'une lanceuse d'alerte doit immédiatement être rapportée via le canal le plus approprié : soit la direction des ressources humaines soit la plateforme de signalement EthicsPoint dont la configuration technique

permet d'empêcher l'accès au contenu des signalements par les personnes nominativement mises en cause.

2.2 Les signalements de représailles font l'objet d'une enquête administrative interne le cas échéant.

2.3 A ce titre tout responsable ou employé qui exerce des représailles contre un autre membre de l'organisation engagé dans une démarche de signalement ou d'alerte est sujet à des mesures disciplinaires, pouvant aller jusqu'à la rupture de contrat.

2.4 Les cas de représailles ou de tentatives avérées de représailles font l'objet d'un rapport aux instances dirigeantes et de contrôle.

NB. Les dispositions anti-représailles ne peuvent être invoquées par des employés sanctionnés pour avoir sciemment formulé de fausses allégations, fourni délibérément des informations trompeuses dans l'intention de nuire ou d'entraver une enquête interne. De même, elles ne peuvent être invoquées par les auteurs d'infraction ou de violations des politiques ou directives institutionnelles et du code de conduite, dans le seul but d'échapper aux sanctions.

3.4 Examen des informations et traitement des cas

Les managers et responsables destinataires du signalement et en charge du traitement des incidents, s'engagent à examiner rapidement tous les signalements. Ils s'engagent à tenir informés les auteurs et autrices des signalements sur l'évolution du dossier, dans la limite de ce qui les concerne personnellement, sur les réponses apportées et les éventuelles mesures d'accompagnement qui seraient décidées¹.

Au terme du processus, les résultats des vérifications ou des enquêtes doivent permettre, selon les cas, soit de clore le dossier sans suite particulière, soit au contraire :

- d'apporter les sanctions éventuelles,
- de mettre en œuvre les mesures de protection et d'accompagnement nécessaires pour les employés, les partenaires ou bénéficiaires exposés ou victimes concernés,
- de prendre les mesures correctives et de protection des intérêts économiques, légaux ou déontologiques de l'association.

¹ Cela étant, les auteurs et autrices d'un signalement ne peuvent en aucun cas exiger d'avoir accès au dossier et à des informations confidentielles. A plus forte raison, aucune information sur l'évolution d'un dossier ne peut être communiquée à des auteurs et autrices de signalements ou à des interlocuteurs et interlocutrices anonymes.

4. Les dispositifs de signalement ouverts à l'externe

En complément des dispositifs internes, destinés aux membres et personnels de l'organisation, d'autres mécanismes peuvent être créés et ouverts à l'externe. C'est notamment le cas sur les terrains d'intervention, où la remontée d'information provenant des bénéficiaires de nos projets ou de nos partenaires est déjà encouragée, dans un but d'évaluation des effets de l'action et d'amélioration de nos prestations.

4.1 Pour les bénéficiaires de nos actions

HI préconise, pour toutes ses missions, la mise en place de dispositifs et d'initiatives d'information, de sensibilisation, de consultation et de recueil des retours (feedbacks) destinés aux bénéficiaires de nos projets. Le but n'est pas seulement d'annoncer et d'accompagner le déroulement des activités, mais aussi de recueillir les opinions, les suggestions, les contributions, les questionnements, voire les inquiétudes ou les doléances.

Par ailleurs, bien que ne relevant pas de notre organisation, l'information issue des initiatives communautaires (comités villageois, de réfugiés, d'usagers, de bénéficiaires), peut enrichir notre analyse des risques et attirer notre attention sur d'éventuels incidents.

4.1.1 Dans les situations de forte exposition aux risques de fraude ou d'abus (situation instable, ampleur des ressources engagées, grande vulnérabilité de catégories particulièrement exposées : femmes, enfants, etc., importance du trafic humain, obstacles au monitoring de l'activité), qui pourraient affecter aussi bien les bénéficiaires que notre organisation, les directeurs, directrices et responsables de la conduite des opérations doivent mettre en place des initiatives spécifiques d'information, de prévention et de recueil des doléances. Ces mesures doivent être planifiées et disposer d'un budget.

4.1.2 Dans tous les cas, il s'agit d'informer les bénéficiaires sur deux points :

- Les conditions de délivrance de l'aide (ex. critères d'éligibilité, nature ou volume de l'aide, modalités concrètes de délivrance, non conditionnalité, ex : gratuité des services, non-discrimination, etc.) ;
- La possibilité offerte de signaler à l'organisation tout manquement, tout entrave, tout abus, dans le respect de la confidentialité.

4.1.3 Ces dispositifs doivent être adaptés (forme et envergure), accessibles (proximité, langue, sans coût significatif pour les usagers) et tenir compte des contraintes culturelles et technologiques. Différentes solutions peuvent être envisagées par les managers de HI, résumées ci-après.

- **Des dispositifs relationnels** : personne identifiée comme point focal, espaces d'accueil, réunions communautaires, groupes de discussion (« focus groups »), entretiens individuels ou sondages, etc.
- **Des dispositifs matériels** : affichage, annonces sonores ou radio, boîtes à suggestions ou à doléances, mise en place d'adresses mail, de numéros téléphoniques, de comptes réseaux sociaux dédiés.

4.2 Pour les organismes partenaires et les fournisseurs

4.2.1 Dans le cadre des relations contractuelles, les organismes partenaires et les entreprises fournissant des biens ou des services doivent également être informés de l'existence de nos politiques, des personnes à contacter et des moyens à utiliser pour signaler et régler tout incident ou litige.

4.2.2 Par conséquent, tous les documents contractuels (accords de partenariat, protocoles d'accord, conditions d'achat, contrats de prestataires de services/fournisseurs) contiennent une référence à nos politiques, un canal de signalement contextualisé et un lien vers la plateforme EthicsPoint.

4.3 Pour les donateurs institutionnels et privés

Pour les donateurs, le canal principal des signalements, réclamations ou plaintes demeure la prise de contact avec les directions et services en charge des relations donateurs au niveau fédéral ou dans les associations nationales de HI.

Cela étant, les donateurs témoins ou victimes d'actes répréhensibles ou de fraudes engageant la réputation de HI peuvent également utiliser la plateforme digitale EthicsPoint.



Signalement des suspicions de fraude ou d'abus

En tant qu'organisation de solidarité internationale engagée pour le respect de la dignité et des droits fondamentaux des personnes handicapées et des populations les plus vulnérables, HI tient non seulement à assurer la protection de ses bénéficiaires, mais aussi celle de toutes les personnes qui sont en contact avec ses actions.

Cette directive présente le cadre général du recueil et du traitement des signalements de suspicions de fraude et d'abus contre les personnes. A ce titre elle intègre les mesures de protection des lanceurs d'alerte et décrit le mécanisme d'alerte professionnelle.

Handicap International – Humanity & Inclusion
69371 Lyon Cedex 08
France
www.hi.org

