Politique dédiée au lancement d'alerte

Template

Pour plus d'information :

contact@whispli.com
www.whispli.com

Notre Modèle de Politique dédiée au Lancement d'Alerte est un outil que vous pouvez utiliser pour prendre une longueur d'avance dans l'élaboration de votre politique interne de lancement d'alerte.

Lors de la création de ce modèle, nous avons examiné les politiques dédiées au lancement d'alerte d'un certain nombre d'organisations. Il s'agit d'entreprises qui ont établi et mis en place des dispositifs de lancement d'alertes efficaces. Cependant, chaque entreprise est différente et chaque organisation doit développer sa propre approche à cet égard. Nous espérons que ce modèle vous fera gagner du temps, vous fournira des idées et vous aidera à développer la meilleure politique dédiée au lancement d'alerte pour votre organisation.

Veuillez noter qu'il s'agit d'un modèle général et que chaque organisation est unique. Son but est de vous fournir des éléments de contenu, de l'inspiration et des meilleures pratiques. A ssurez-vous de consulter vos experts internes, y compris vos équipes juridiques et de ressources humaines, pour rédiger une politique dédiée au lancement d'alerte adaptée aux besoins spécifiques de votre organisation.

Ce modèle couvrira les rubriques et sections suivantes :

Section 1 : Notre objectif

1.1 Nos objectifs et notre engagement

La vision de {Insérer Nom de l'Entreprise} est {Insérer Vision de l'Entreprise}. Pour réaliser notre vision, il est crucial que tous nos employés et partenaires comprennent, suivent et adhèrent à nos valeurs d'entreprise {Insérez vos valeurs d'entreprise ici}. Nous avons mis en place des lignes directrices et des politiques pour nous assurer que nous vivons selon ces valeurs dans notre travail quotidien.

Parallèlement à nos valeurs, nous voulons avoir un retour d'information et encourager les personnes à s'exprimer lorsqu'elles sont témoins d'activités ou de comportements qu'ils jugent répréhensible ou ne correspondant pas à nos valeurs.
L'objectif de cette politique est de fournir des directives très claires sur la façon dont nous abordons et gérons ces alertes. Avec notre politique dédiée au lancement d'alerte, nous visons à garantir :

- Chaque employé doit avoir la possibilité de s'exprimer de manière anonyme lorsqu'il estime que nos valeurs d'entreprise ne sont pas respectées. Ils doivent disposer d'un endroit pour signaler les fautes. Chaque alerte sera entendue et traitée, et nous nous engageons à apporter les améliorations nécessaires relatives aux résultats de l'enquête conduite.

- {Insérer le Nom de l'Entreprise} pense que tout le monde devrait pouvoir lancer une alerte de manière anonyme. Nous nous engageons à protéger l'identité des lanceurs d'alerte, et la décision de révéler leur identité leur appartient entièrement.

- Nous enquêterons sur chaque signalement d'irrégularité. À la fin de l'enquête, nous documenterons les résultats et fournirons un compte rendu, le cas échéant.

1.2 Notre engagement

{Insérer le Nom de l'Entreprise} souhaite que ses employés se sentent en mesure de fournir des informations sur leurs préoccupations, qu'ils comprennent où ils peuvent effectuer leurs

alertes, qu'ils aient connaissance des étapes suivant leur alerte et s'assurer qu'ils se sentent en sécurité en lançant une alerte. {Insérer le Nom de l'Entreprise} souhaite également les informer de leur droit à l'anonymat et de la manière dont nous, en tant qu'organisation, veillerons à ce qu'ils ne fassent l'objet d'aucune représailles ou d'autres abus en raison de leur signalement.

1.3 Quels comportements doivents être signalés

Il est important que {Insérer le Nom de l'Entreprise} définisse les comportements que nous souhaitons voir signalés dans le cadre de cette politique. Nous souhaitons vous entendre si vous êtes témoin ou avez connaissance d'un comportement qui est :

- Frauduleux ;
- Illégal ;
- Corrompu ;
- Malhonnête ;
- Contraire à l'éthique ;
- Viole la loi ou tout autre code juridique ;
- Crée un environnement dangereux ;
- Enfreint l'une des politiques de notre entreprise ;
- Discriminant ;
- Relève du harcèlement et/ou intimidation de toute sorte ;
- Toute conduite préjudiciable à {Insérer Nom de l'Entreprise} et susceptible d'entraîner une perte financière ou non financière ;

1.4 Qui est concerné par cette politique ?

Les personnes suivantes seraient considérées comme une « personne éligible » et seraient concernées par la politique dédiée au lancement d'alerte de {Insérer le Nom de l'Entreprise}.

- Employés (dont directeurs, managers, stagiaires et intérimaires) ;
- Entrepreneurs, consultants, prestataires de services, fournisseurs, partenaires commerciaux ;
- Anciens salariés ;

{Insérez toute autre personne éligible en fonction de vos pratiques commerciales, de vos opérations, de votre organisation, de votre structure organisationelle, etc.}

Cette politique s'applique à toutes les entreprises, divisions et bureaux de {Insérer le Nom de l'Entreprise}. Elle s'applique également dans toutes les juridictions où nous opérons. Si la législation, la réglementation ou les lois locales offrent un niveau de protection supérieur à celui inclus dans cette politique, la législation locale prévaudra.

Section 2 : Processus de lancement d'alerte

2.1 Quelles options les employés ont-ils pour lancer une alerte

Si un employé ou une personne éligible souhaite lancer une alerte, il dispose de différents canaux pour le faire. Des instructions détaillées sur la façon d'utiliser et d'aborder chacun de ces canaux sont incluses dans l'Annexe 1.

- Alerte/signalement anonyme via le Web et mobile {Lien vers votre dispositif d'alerte interne} ;
- E-mail anonyme {listez l'e-mail anonyme ici} ;
- Via la hotline des employés {indiquez le numéro de téléphone ici} ;
- Par la poste {indiquez l'adresse ici} ;
- Parler à un cadre supérieur chez {Insérer le Nom de l'Entreprise} ;
- Parler avec la personne en charge du dispositif d'alerte de {Insérer le Nom de l'Entreprise} ;

{Utilisez cette section pour répertorier tous les canaux supplémentaires que vous fournissez aux employés pour soumettre des alertes ou des alertes anonymes. Des exemples supplémentaires pourraient être le chat en direct, les SMS, la messagerie vocale via la hotline, le fax, etc.}

2.2 Vous pouvez rester anonyme

{Insérer le Nom de l'Entreprise} respecte et protège votre identité si vous choisissez de faire un signalement anonyme. Vous pouvez choisir de rester anonyme lors de la rédaction d'un

rapport d'alerte, de l'interaction avec les gestionnaires de cas lors d'une enquête sur votre alerte, ainsi qu'après la clôture de votre dossier. À tout moment, vous pouvez vous identifier, mais ce choix vous appartient et à aucun moment vous n'avez besoin de le faire ou vous ne serez obligé de fournir votre identité.

Si vous décidez de divulguer votre identité, {Insérer le Nom de l'Entreprise} s'efforcera de la protéger et indiquera et documentera qui, au sein de l'organisation, saura que vous avez soumis votre rapport d'alerte. {Insérer le Nom de l'Entreprise} prendra également toutes les mesures nécessaires (et décrites dans cette politique) pour s'assurer que vous ne subissez aucune représailles.

Il convient de noter que {Insérer le Nom de l'Entreprise} fera tout son possible pour enquêter sur votre alerte, mais dans certains cas, il y a des limites à ce qui peut être réalisé si le lanceur d'alerte décide de rester anonyme.

2.3 En quoi consiste le processus d'enquête ?

Il est important pour {Insérer le Nom de l'Entreprise} d'être transparent avec nos employés et de décrire la procédure à suivre pour enquêter sur une alerte soumise via nos canaux de signalisation. Ci-dessous, nous avons fourni les différentes étapes qu'un gestionnaire de cas ou un membre de notre équipe en charge des signalements suivra une fois qu'un rapport est reçu jusqu'à ce que le dossier soit clos.

{Insérez votre processus d'enquête général sous forme de points clés. Vous trouverez ci-dessous un exemple de ce qui doit être détaillé dans votre politique dédiée au lancement d'alerte.}

- Le rapport d'alerte (anonyme ou non) est reçu.
- Un gestionnaire de cas est affecté au rapport pour l'évaluer et confirmer sa réception.
- Le gestionnaire de cas effectuera une évaluation initiale pour confirmer qu'il s'agit d'une alerte valide et demandera l'autorisation d'enquêter.
- Le gestionnaire de cas commencera son enquête. Cela peut inclure la correspondance avec l'informateur s'il existe un canal pour le faire.
- Le gestionnaire de cas enquêtera et informera la direction et le lanceur d'alerte conformément aux directives de la politique.

- Une fois que le gestionnaire de cas a finalisé son enquête et son rapport, la direction et le lanceur d'alerte seront informés.
- À ce stade, le gestionnaire de cas remettra le tout à la direction pour qu'elle prenne les mesures qui s'imposent.

2.4 Comment faisons-nous appel à des tiers

Chez {Insérer le Nom de l'Entreprise}, nous utilisons des tiers dans notre programme et notre stratégie d'alerte interne. Voici des exemples de la manière dont nous pourrions utiliser des tiers :

{Modifiez cette partie pour l'adapter à la façon dont votre organisation utilise des tiers dans le cadre de votre dispositif d'alerte interne}

- Plate-forme de lancement d'alerte : {Insérer le Nom de l'Entreprise} utilise une plate-forme de lancement d'alerte tierce, {Insérez son nom ici}, pour s'assurer que nous protégeons l'identité des lanceurs d'alerte et tirons parti des technologies pour garantir que personne dans notre organisation ne puisse les identifier. Cette plate-forme permet également une communication bidirectionnelle anonyme ainsi que des fonctionnalités de gestion de cas et de protection des données.
- Cabinets comptables : {Insérer le nom de l'entreprise} fait appel à des cabinets comptables tiers pour mener des enquêtes judiciaires sur des alertes spécifiques provenant de notre dispositif d'alerte.
- Cabinets d'enquête : {Insérer le Nom de l'Entreprise} fait appel à des cabinets d'enquête spécialisés pour enquêter sur des cas spécifiques pour lesquels nous ne disposons pas des compétences nécessaires en interne. Ils sont également utilisés pour les enquêtes que nous préférerions qu'un tiers exécute en raison de la nature de l'alerte.
- Consultants en ressources humaines : {Insérer le Nom de l'Entreprise} fait appel à des consultants en ressources humaines dans l' ensemble de notre entreprise et ils peuvent être impliqués dans des cas d'alertes spécifiques, garantissant que nous utilisons les meilleures pratiques en matière de ressources humaines lorsque nous évaluons, enquêtons et prenons des mesures.

2.5 Qui est informé d'une alerte

Une fois qu'une alerte est soumise (anonyme ou non), cette alerte est envoyée à {Insérer le rôle du destinataire}. Cette personne évaluera ensuite le rapport de l'alerte et l'attribuera à un gestionnaire de cas, qui gérera l'enquête.

Certains cadres supérieurs pourraient être informés de l'alerte dans le cadre du processus de lancement d'alerte, ou s'ils sont impliqués dans l'enquête d'une manière ou d'une autre.

Toute information susceptible d'identifier un lanceur d'alerte anonyme sera tenue dans la plus stricte confidentialité et ne sera pas partagée, à moins que {Insérer le Nom de l'Entreprise} n'y soit contraint par la loi.

2.6 Quel est le processus de retour d'information au lanceur d'alerte

Dans le cadre de notre processus d'enquête, {Insérer le Nom de l'Entreprise} informera le lanceur d'alerte de l'avancement de l'enquête. Ces mises à jour peuvent inclure les éléments suivants :

- {Insérer le Nom de l'Entreprise} a confirmé la réception de l'alerte.
- {Insérer le Nom de l'Entreprise} a commencé le processus d'enquête.
- L'enquête est actuellement en cours.
- L'enquête est close.

L'engagement de {Insérer le Nom de l'Entreprise} est que le lanceur d'alerte sera informé une fois par mois pendant que l'enquête est en cours. Il sera ensuite notifié une fois l'enquête clôturée.

{Insérer le Nom de l'Entreprise} s'efforcera de fournir autant de commentaires que possible sur l'enquête. Cependant, en raison des directives de confidentialité de {Insérer le Nom de l'Entreprise}, il arrive souvent que des informations ne puissent pas être partagées avec le lanceur d'alerte.

2.7 Que faire si le lanceur d’alerte n'est pas satisfait du résultat

Si, après avoir reçu le rapport résumé de l'enquête, le lanceur d’alerte n'est pas satisfait du résultat, il peut le signaler à {Insérer le rôle de la personne en charge de votre dispositif d’alerte interne}. Le lanceur d’alerte peut fournir cette escalation par écrit afin qu'un examen formel puisse avoir lieu. Bien que {Insérez le rôle de la personne en charge de votre dispositif d’alerte interne} s'engage à examiner la demande, {Insérer le Nom de l’Entreprise} n'a aucune obligation de rouvrir l'enquête. Si {Insérez le rôle de la personne en charge de votre dispositif d’alerte interne} conclut que l'enquête a été menée correctement et qu'il n'existe aucune nouvelle information susceptible de modifier les résultats de l'enquête, l'enquête sera close.

Section 3 : Comment les lanceurs d’alerte sont protégés

3.1 Anonymat après avoir lancé une alerte

Section 2.2 a détaillé comment une personne éligible peut rester anonyme pendant le processus de lancement d’une alerte. Après avoir soumis un rapport, les politiques suivantes concernant l'anonymat sont en place pour protéger l'identité d'un lanceur d’alerte.

- Le lanceur d’alerte a le droit de rester anonyme et n'a besoin de s'identifier à aucun moment pendant le processus d'enquête.
- {Insérer le Nom de l’Entreprise} utilise des outils et des plates-formes qui aident à protéger l'identité d'un lanceur d’alerte pendant et après la soumission d'une alerte.
- {Insérer le Nom de l’Entreprise} ne forcera à aucun moment le lanceur d’alerte à révéler son identité.
- Le lanceur d’alerte peut refuser de répondre aux questions s'il pense qu’elles peuvent l'identifier.
- Si le lanceur d’alerte décide de révéler son identité à tout moment au cours du processus, vous documenterez qui aura accès à son identité. Cela peut inclure le gestionnaire de cas, le responsable du dispositif d’alerte etc.

3.2 Représailles potentielles

Un lanceur d'alerte peut craindre que le personnel, la direction ou l'organisation n'exerce des représailles à son encontre. Dans ce cas, {Insérer le Nom de l'Entreprise} protégera le lanceur d'alerte contre :
{Modifiez pour représenter la protection potentielle qui sera offerte à un employé.}

- Licenciement ou cessation d'emploi ;
- Gestion des performances ;
- Harcèlement ou intimidation sur le lieu de travail;
- Avertissements ou actions disciplinaires ;
- Discrimination ;
- Toute autre action pouvant être perçue comme des représailles pour avoir lancé une alerte ;

3.3 Risque estimé de représailles

Dans le cas d'un « risque estimé de représailles », le lanceur d'alerte pense que des représailles sont proches ou imminentes et qu'il est ciblé par celles-ci. En cas de représailles estimées, le lanceur d'alerte doit contacter le {Insérer le rôle de la personne en charge de votre dispositif d'alerte interne}.
Le {Insérer le rôle de la personne en charge de votre dispositif d'alerte interne} prendra les mesures qu'il juge appropriées et proposera des recommandations sur la manière de résoudre la situation. Les mesures potentielles pour protéger le lanceur d'alerte d'un risque estimé de représailles peuvent inclure :

- Le congé du lanceur d'alerte.
- Le lanceur d'alerte est réaffecté à d'autres tâches.
- Le lanceur d'alerte est réaffecté à un autre emplacement.

3.4 Déjà victime de représailles

Si le lanceur d'alerte estime qu'il a déjà fait l'objet de représailles, il doit le signaler immédiatement au {Insérer le rôle de la personne en charge de votre dispositif d'alerte}. Le {Insérer le rôle de la personne en charge de votre dispositif d'alerte} prendra les mesures qu'il juge appropriées et proposera des recommandations sur la manière de résoudre la

situation. Les mesures potentielles pour protéger le lanceur d'alerte après que des représailles se sont produites peuvent inclure :

- Le congé du lanceur d'alerte.
- Le lanceur d'alerte est réaffecté à d'autres tâches.
- Le lanceur d'alerte est réaffecté à une autre localisation.

3.5 Représailles non résolues de manière adéquate

Si le lanceur d'alerte estime que son rapport signalant des représailles n'a pas été résolu de manière adéquate, il peut escalader ce cas par écrit. Le rapport devra être envoyé à {Insérer le rôle de la personne en charge de votre dispositif d'alerte ou du département auquel vous souhaitez que ces rapports soient transmis}, ils enquêteront sur l'affaire et évalueront la manière dont les représailles ont été traitées.

3.6 Comment {insérer le nom de l'entreprise} traite les représailles

{Insérer le Nom de l'Entreprise} ne tolère aucune tentative de représailles contre un lanceur d'alerte qui a effectué un signalement. Tout employé ou personne associée qui s'est rendu coupable de représailles s'exposera à des mesures disciplinaires, y compris la possibilité d'être licencié de ses fonctions.

3.7 Séparation des problèmes

{Insérer le Nom de l'Entreprise} sera en mesure de soulever tout problème lié au travail ou aux performances. Bien que {Insérer le Nom de l'Entreprise} protège le lanceur d'alerte de toute représailles, il est également important qu'il soit toujours efficace dans son travail. {Insérer le Nom de l'Entreprise} peut toujours soulever des problèmes de performance ou de contrat avec le lanceur d'alerte tant qu'ils sont séparés et qu'ils ne sont pas influencés par les alertess qui ont été lancées.

3.8 Protection et immunité des autres parties

Les autres parties qui pourraient avoir à témoigner ou qui sont impliquées dans l'enquête seront protégées contre les représailles de la même manière que le lanceur d'alerte.

3. 9 Protection et assistance législative/réglementaire

Si, dans une juridiction ou un lieu où {Insérer le Nom de l'Entreprise} opère, des lois de protection relatives aux signalements offrent un niveau de protection supérieur à celui inclus dans cette politique, la législation locale prévaudra.

Section 4 : Nos rôles et responsabilités

4.1 Rôles

Les rôles au sein du dispositif d'alerte de {Insérer le Nom de l'Entreprise} incluent les éléments suivants :

{Veuillez insérer les rôles spécifiques que vous avez dans votre organisation. Il s'agit des dénominations courantes uniquement.}

- Propriétaire et responsable du dispositif d'alerte et responsable de la protection relative aux alertess (WPO) ;
- Responsable au quotidien du dispositif d'alerte de {Insérer le Nom de l'Entreprise} ;
- Les gestionnaires de cas qui enquêtent sur les rapports d'alertes individuels ;
- Ressources humaines impliquées dans les dossiers et sensibilisées aux enquêtes spécifiques ;

4.2 Responsabilités

Voici les responsabilités de chaque rôle au sein du dispositif d'alerte interne de {Insérer le Nom de l'Entreprise}.

{Veuillez insérer les responsabilités spécifiques que vous avez dans votre organisation. Il s'agit des dénominations courantes uniquement.}

- Propriétaire du dispositif/agent de protection relative aux alertes : cet individu est propriétaire de l'ensemble du dispositif d'alerte interne et est évalué en fonction de son succès global. Cela inclut la connaissance et la compréhension du dispositif par les employés, un processus simple pour soumettre une alerte, l'enquête réalisée sur les alertes reçues, ainsi qu'être un point d'escalade pour toute préoccupation ou représaille aillant lieu. Bien que cette personne relève de l'organisation, les résultats de son travail vont directement au conseil d'administration.

- Gestionnaire journalier : le gestionnaire journalier visualise les alertes anonymes entrantes, attribue ces rapports aux gestionnaires de cas et les gère pendant qu'ils mènent des enquêtes. Cette personne est la première ligne d'escalade et travaille en collaboration avec les gestionnaires de cas pour s'assurer que les alertes anonymes sont entendus et traitées.

- Gestionnaires de cas : les gestionnaires de cas se voient attribuer des alertes anonymes et leur rôle est d'enquêter sur ces rapports. Cela comprend interagir et poser des questions aux lanceurs d'alerte, ainsi que l'utilisation des informations fournies pour enquêter sur le rapport soumis. Leur enquête peut être interne ou externe à l'organisation selon ce qui a été documenté dans le rapport de l'alerte. Leur objectif est de rassembler les faits et de présenter un rapport final à la direction sur ce qui s'est passé et sur les mesures qu'ils jugent nécessaires.

- Ressources humaines : Des collègues des ressources humaines peuvent être appelés à fournir des conseils et des orientations lors d'une enquête. Le dispositif d'alerte interne s'appuie sur leur expertise et leur perspicacité pour s'assurer que {Insérer le Nom de l'Entreprise} utilise les meilleures pratiques RH au cours des enquêtes et que nous traitons tous les employés équitablement.

Section 5 : Gouvernance

5.1 Modifications de la politique dédiée au lancement d'alerte de {insérer le nom de l'entreprise}

De temps à autre, la politique dédiée au lancement d'alerte de {Insérer le Nom de l'Entreprise} devra être modifiée pour suivre nos valeurs, nos meilleures pratiques, nos améliorations ainsi que la législation et réglementation.
Toute modification de notre politique dédiée au lancement d'alerte sera communiquée à tous les employés et à toutes les parties prenantes concernées. Cette politique et toute modification apportée constituent un contrat de travail.

Toute modification de la politique dédiée au lancement d'alerte de {Insérer le Nom de l'Entreprise} doit être approuvée par :
- le PDG
- le responsable de la conformité
- le propriétaire du dispositif d'alerte interne de {Insérer le Nom de l'Entreprise}

Toutes les modifications seront examinées par le conseil d'administration et le conseil peut commenter et faire remonter des informations si nécessaire. Tous les changements seront également documentés dans la politique dédiée au lancement d'alerte de {Insérer le Nom de l'Entreprise} et seront mis à la disposition de tous les employés.

5.2 Rapports au Conseil d'administration

Le Conseil d'administration est informé chaque trimestre sur le dispositif d'alerte interne de {Insérer le Nom de l'Entreprise}, y compris les alertes, les enquêtes et les résultats. Les alertes ou les enquêtes comportant un risque excessif seront signalés au conseil d'administration en dehors des mises à jour trimestrielles. Le conseil d'administration peut à tout moment poser des questions sur les alertes anonymes, les enquêtes, ainsi que sur l'état du dispositif d'alerte interne de {Insérer le Nom de l'Entreprise}.

Le dispositif d'alerte interne de {Insérer le Nom de l'Entreprise} réside dans le comité de conformité du conseil d'administration. Ils sont responsables de la mise en œuvre et l'efficacité du dispositif d'alerte interne de {Insérer le Nom de l'Entreprise}.

Annexe 1 : Canaux de signalement

{Documenter en détail comment un employé peut vous soumettre une alerte, en énumérant tous les canaux et étapes (ou liens vers les étapes) pour faire un rapport}.

Annexe 2 : Registre des modifications

{Documentez toutes les modifications apportées à votre politique dédiée au lancement d'alerte}.

Annexe 3 : Toutes les lois/réglementations locales pertinentes

{Documentez toute législation ou réglementation locale qui affecte ou régit la dénonciation dans les juridictions où vous opérez. Cela peut être à la fois au niveau de l'État ou au niveau national selon les pays où vos employés sont basés.}