SANIPOD

RAPPORT SUR L'ÉTHIQUE **DES AFFAIRES**

- 2025 -

TABLE DES MATIÈRES

I – OBJECTIFS ET PORTÉE

La présente **Politique d'éthique des affaires** a pour objectif de formaliser les engagements de Chaussures de la Bièvre en matière d'intégrité, de conformité et de responsabilité.

Cette politique constitue un socle de valeurs partagées et de règles de conduite destinées à guider tous les acteurs de l'entreprise dans leurs décisions et leurs comportements quotidiens. Elle vise à prévenir tout manquement éthique, à promouvoir une culture de transparence et à garantir que nos activités respectent les lois, les réglementations, ainsi que les engagements volontaires auxquels nous souscrivons.

Sanipod s'engage à maintenir les plus hauts standards en matière d'éthique professionnelle, notamment en matière de lutte contre la corruption, de prévention des conflits d'intérêts, de lutte contre la fraude, de sécurité de l'information et de protection des données.

La Politique d'éthique des affaires de Sanipod s'applique à l'ensemble des personnes et entités agissant pour ou au nom de l'entreprise, à savoir :

- Tous les collaborateurs, quel que soit leur niveau hiérarchique ;
- Les fournisseurs, prestataires et autres partenaires commerciaux ou institutionnels.

L'ensemble de ces parties est tenu de respecter les principes énoncés dans cette politique. Le non-respect des dispositions peut entraîner des mesures disciplinaires, contractuelles ou légales, selon les cas.

II – PRINCIPES ÉTHIQUES FONDAMENTAUX

A) Valeurs et principes clés

Chez Sanipod, notre vision de l'éthique repose sur un ensemble de **valeurs fondamentales** qui inspirent nos comportements, nos décisions et nos relations internes et externes. Ces principes guident notre conduite au quotidien et renforcent la crédibilité de notre entreprise auprès de l'ensemble de nos parties prenantes.

Intégrité

Nous agissons avec honnêteté, transparence et rigueur, en toutes circonstances. Nous refusons toute forme de manipulation, de dissimulation ou de malhonnêteté, tant en interne qu'en externe.

Responsabilité

Chaque collaborateur est responsable de ses actes et de leurs conséquences sur l'entreprise, ses collègues, ses partenaires et la société dans son ensemble. Nous nous

engageons à respecter les lois, les règles internes et les engagements volontaires que nous prenons.

Respect
Nous favorisons un climat de travail fondé sur le respect mutuel, la dignité, la diversité et l'inclusion. Ce principe s'applique à toutes nos interactions, que ce soit avec des collègues, des clients, des fournisseurs ou d'autres parties prenantes.

Exemplarité
Les dirigeants et managers de Sanipod ont une responsabilité particulière : celle d'incarner ces valeurs au quotidien et de montrer l'exemple en matière d'éthique et de conformité.

Transparence
Nous communiquons de manière claire, complète et sincère. Nous encourageons la remontée d'informations et la mise en lumière des problèmes, dans une logique de progrès et d'amélioration continue.

Équité
Nous agissons de manière juste et impartiale dans la prise de décision, sans favoritisme ni discrimination. Les décisions doivent être basées sur des critères objectifs, dans le respect de l'intérêt général de l'entreprise.

B) Comportement éthique attendu

Tous les collaborateurs et partenaires de Sanipod sont tenus d'adopter un comportement irréprochable dans l'exercice de leurs fonctions. Le respect des règles éthiques n'est pas une option : il constitue une exigence fondamentale et permanente dans toutes nos activités.

Respect des lois et réglementations
Chaque collaborateur doit se conformer à l'ensemble des lois, règlements, normes professionnelles et conventions applicables à son activité, en France comme à l'international.
Cela comprend notamment :

- Les règles en matière de droit du travail, de concurrence, de fiscalité, d'environnement, de protection des données personnelles ;
- Les législations relatives à la corruption, au blanchiment d'argent, à la fraude et à la sécurité informatique.

Utilisation responsable des ressources de l'entreprise
Les biens, équipements, outils informatiques et ressources de Sanipod doivent être utilisés exclusivement dans un cadre professionnel, avec loyauté et souci de préservation.

Relations professionnelles éthiques
Les relations avec les collègues, clients, fournisseurs, prestataires et autres parties prenantes doivent être empreintes de courtoisie, d'équité, de professionnalisme et de respect mutuel. Aucun comportement discriminatoire, harcelant, abusif ou irrespectueux ne saurait être toléré.

Communication transparente et sincère
Les informations échangées, en interne comme en externe, doivent être exactes, complètes, compréhensibles et délivrées de bonne foi. La manipulation d'informations ou la rétention volontaire de faits essentiels est proscrite.

Prévention des conflits d'intérêts
Les collaborateurs doivent éviter toute situation dans laquelle leur intérêt personnel pourrait interférer avec l'intérêt de l'entreprise. Les conflits d'intérêts réels, potentiels ou apparents doivent être signalés sans délai selon les procédures prévues.

Refus des pratiques non éthiques
Aucun collaborateur ne doit accepter ou proposer un avantage indu (cadeau, invitation, paiement, etc.) qui pourrait influencer de manière inappropriée une décision professionnelle. Les pratiques de corruption, de fraude ou de favoritisme sont strictement interdites.

III – POLITIQUE DE LUTTE CONTRE LA CORRUPTION

A) Engagement de l'entreprise

Sanipod adopte une **tolérance zéro à l'égard de toute forme de corruption**, qu'elle soit active ou passive, publique ou privée, en France comme à l'international. Cet engagement vise à préserver l'intégrité de l'entreprise, à renforcer la confiance de ses parties prenantes et à se conformer strictement aux dispositions légales, notamment la loi Sapin II, le Code pénal et les conventions internationales anticorruption.

Définitions :
· **Corruption active** : offrir, promettre ou accorder un avantage indu à une personne dans le but d'obtenir un traitement favorable.
· **Corruption passive** : solliciter ou accepter un avantage en échange d'une décision favorable, réelle ou attendue.
· **Influence indue** : obtenir un avantage en utilisant son pouvoir ou ses relations pour influencer une décision, même indirectement.

Les collaborateurs et partenaires de Sanipod ne doivent :
· Offrir, promettre, donner ou accepter des cadeaux, paiements, invitations ou avantages qui pourraient être perçus comme des tentatives d'influence ;

- Verser des paiements de facilitation (même modestes) à des agents publics pour accélérer une procédure administrative ;
- Utiliser des intermédiaires pour dissimuler des pratiques de corruption ;
- Dissimuler des paiements ou transactions dans les livres comptables.

Cadeaux et invitations :
Des cadeaux ou invitations peuvent être acceptés ou offerts uniquement s'ils répondent à tous les critères suivants :
- Sont de valeur modérée ;
- Sont ponctuels et exceptionnels ;
- Ne cherchent pas à influencer une décision ;
- Sont conformes aux usages professionnels et culturels locaux.

Tout doute doit être soumis à la direction.

B) Cartographie des risques de corruption

Dans le cadre de sa politique de conformité, Sanipod met en œuvre une **cartographie des risques de corruption**. Cet outil stratégique permet d'identifier, d'évaluer et de maîtriser les risques auxquels l'entreprise peut être exposée dans le cadre de ses activités.

Examen périodique des risques :
La cartographie fait l'objet d'une mise à jour régulière lors de tout changement significatif dans l'organisation, les activités, les marchés ou la réglementation et à la suite d'un incident ou d'une alerte mettant en évidence un nouveau risque.

Description des risques identifiés :

Zone	Risque principal	Niveau	Actions clés
Production	Favoritisme ou dépendance à certains fournisseurs	Élevé	Séparation des rôles, dossiers fournisseurs, clauses contractuelles
Choix des matériaux	Collusion pour imposer des matériaux coûteux ou douteux	Moyen	Validation technique et budgétaire documentée
Points de vente	Avantages indus pour obtenir de bons emplacements	Moyen	Contrats, validation juridique, revue des avantages
Canal B2B (revendeurs)	Remises ou accords non officiels contre avantages personnels	Moyen	Contrats écrits, contrôle des signatures, double validation
Relations presse / marketing	Invitations ou cadeaux mal encadrés	Faible	Politique de cadeaux, traçabilité, validation hiérarchique

Magasin d'usine (Sillans)	Favoritisme local ou arrangements informels	Faible	Procédures de caisse, supervision, audits ponctuels
Logistique / stocks	Détournements ou arrangements avec des transporteurs	Moyen	Contrôles réguliers, inventaires, sous-traitants référencés
Cadeaux & invitations	Dépassement des limites acceptables	Faible	Plafonnement, déclaration obligatoire, registre centralisé

Plan d'actions correctives associé :

Mesures	Statut
Formalisation d'une procédure de sélection des fournisseurs clés	En place
Intégration de clauses anti-corruption dans tous les contrats	En place
Registre centralisé des cadeaux et invitations	À mettre en place
Formation des fonctions exposées (achats, ventes, logistique)	À mettre en place
Audit annuel des points de vente et des stocks	À mettre en place

IV – POLITIQUE EN MATIÈRE DE CONFLITS D'INTÉRÊTS

A) Définition d'un conflit d'intérêts

Un conflit d'intérêts survient lorsqu'un collaborateur ou un partenaire commercial se trouve dans une situation où son intérêt personnel (ou celui d'un proche) pourrait interférer avec l'intérêt de l'entreprise ou influencer sa capacité à prendre une décision impartiale, objective et professionnelle.

B) Obligations des collaborateurs

Tout collaborateur a le devoir de :

- Éviter activement toute situation pouvant donner lieu à un conflit d'intérêts ;
- Déclarer sans délai à son supérieur hiérarchique ou au référent éthique toute situation réelle, potentielle ou apparente ;
- S'abstenir de toute décision ou participation à un processus concerné tant que la situation n'a pas été évaluée et tranchée.

C) Procédure de déclaration et de traitement

1. Déclaration :

- Le collaborateur transmet la déclaration de conflit d'intérêts au référent éthique via l'adresse mail suivante : ***olivier.richard@hardrige.com***.
- La déclaration précise la nature du conflit, les parties concernées et les faits.

2. Évaluation :

- La direction générale analyse la situation et détermine les mesures à prendre.

3. Mesures possibles :

- Recadrage des missions ;
- Retrait temporaire du collaborateur d'un processus décisionnel ;
- Remplacement du collaborateur sur une tâche sensible.

Aucune mesure de représailles ne sera prise à l'encontre d'un collaborateur ayant signalé de bonne foi un conflit d'intérêts. L'ensemble des déclarations est traité de manière confidentielle et proportionnée.

V. POLITIQUE EN MATIÈRE DE FRAUDE

A) Définition de la fraude

La fraude désigne tout acte intentionnel destiné à tromper, détourner ou manipuler des ressources ou des informations dans le but d'en retirer un avantage personnel ou de porter préjudice à l'entreprise. Elle peut être le fait d'un collaborateur, d'un partenaire externe ou d'un tiers.

Elle peut notamment se manifester par :

- La falsification de documents comptables ou commerciaux ;
- Le détournement de stocks, d'espèces ou de marchandises ;
- La manipulation des données de facturation ;
- L'abus de pouvoir ou de position pour obtenir des avantages indus ;
- La déclaration mensongère dans le cadre d'une procédure interne.

B) Engagement de l'entreprise

Sanipod adopte une tolérance zéro envers toute forme de fraude, qu'elle soit commise en interne ou en externe. L'entreprise s'engage à :

- Détecter rapidement les comportements frauduleux ;
- Les traiter avec rigueur et impartialité ;
- Engager, le cas échéant, des poursuites disciplinaires, civiles ou pénales ;
- Renforcer la culture de l'intégrité et des contrôles.

C) Dispositifs de prévention, détection et signalement

- Séparation des tâches critiques (achats, validation, paiement) ;
- Vérification des flux financiers et physiques (stock, caisse, remises) ;
- Vérifications croisées dans les services sensibles

Tout collaborateur ou partenaire peut signaler de bonne foi une suspicion de fraude via un mail au référent éthique ***olivier.richard@hardrige.com***. Les signalements seront traités avec confidentialité, objectivité et sans représailles à l'égard du lanceur

d’alerte.

VI – POLITIQUE DE LUTTE CONTRE LE BLANCHIMENT D’ARGENT

A) Définition du blanchiment d’argent

Le blanchiment d’argent consiste à dissimuler l’origine illicite de fonds obtenus à la suite d’activités criminelles (fraude fiscale, corruption, trafic, etc.), en les réinjectant dans le circuit économique légal. Cette pratique inclut également le financement du terrorisme lorsqu’elle sert à financer des actes violents à des fins politiques ou idéologiques.

Bien que Sanipod évolue dans un secteur à risque modéré, elle reste exposée à certaines situations sensibles dans le cadre de ses transactions B2B, de ses relations internationales, ou via des partenaires externes.

B) Engagement de l’entreprise

Sanipod s’engage à refuser toute opération suspecte, à coopérer avec les autorités compétentes et à mettre en place des dispositifs de vigilance adaptés afin de prévenir tout usage abusif de ses circuits financiers ou logistiques.

Chaque collaborateur manipulant des fonds, validant des paiements ou gérant des relations avec des tiers a l’obligation :

- De faire preuve de vigilance raisonnable ;
- De signaler sans délai toute opération suspecte ou douteuse.

C) Mesures de prévention et de signalement mises en œuvre

- Identification préalable des clients et partenaires avant tout engagement ;
- Vérification des bénéficiaires effectifs des sociétés partenaires ;
- Interdiction des paiements en espèces supérieurs aux seuils légaux ;
- Contrôle renforcé sur les transactions inhabituelles, notamment lors d’exportations ou remises exceptionnelles ;

Toute suspicion de blanchiment d’argent ou de transaction irrégulière doit être immédiatement signalée à l’adresse mail ***olivier.richard@hardrige.com***, qui pourra :

- Suspendre la transaction en attente de vérifications ;
- Contacter les autorités compétentes si nécessaire.

VII – POLITIQUE RELATIVE À LA SÉCURITÉ DE L'INFORMATION

A) Engagement de l'entreprise

La sécurité de l'information est essentielle pour protéger les données stratégiques, commerciales et personnelles traitées par Sanipod. Cette politique vise à :

- Garantir la confidentialité, l'intégrité et la disponibilité des informations ;
- Protéger l'entreprise contre les fuites de données, cyberattaques, pertes accidentelles ou usages non autorisés ;
- Se conformer aux obligations légales (notamment le RGPD).

Elle s'applique à l'ensemble des collaborateurs, prestataires, sous-traitants et toute personne ayant accès aux systèmes d'information de l'entreprise.

B) Évaluations des risques liés à la sécurité de l'information

L'évaluation régulière des risques liés à la sécurité de l'information permet à Sanipod de :

- Identifier les vulnérabilités potentielles dans ses systèmes et processus ;
- Anticiper les menaces internes ou externes (erreurs humaines, cyberattaques, fuites de données, etc.) ;
- Adapter ses mesures de protection et renforcer sa résilience numérique.

Examen périodique des risques :

La cartographie fait l'objet d'une mise à jour régulière lors de tout changement significatif dans l'organisation, les activités, les marchés ou la réglementation et à la suite d'un incident ou d'une alerte mettant en évidence un nouveau risque.

Principaux risques identifiés :

Actif / Processus	Risque principal	Niveau	Mesures clés
Données clients	Fuite ou perte de données personnelles	Élevé	Authentification forte, sauvegardes, accès limités
Stocks & commandes	Données faussées ou supprimées	Moyen	Double validation, alertes automatiques
Postes utilisateurs	Vol ou piratage de postes	Élevé	Mots de passe, verrouillage auto, sensibilisation
Messagerie pro	Phishing ou fuite par email	Élevé	Filtres anti-phishing, formations, vérifications manuelles
Partage de fichiers / cloud	Mauvais paramétrage ou stockage non sécurisé	Moyen	Limitation des outils autorisés
Fournisseurs IT / services	Dépendance critique à des prestataires	Moyen	Clauses RGPD, audits, plans de secours
Données RH & paye	Accès non autorisé à des données sensibles	Moyen	Accès restreint, suivi des accès, confidentialité

Plan d'actions correctives :

Risque prioritaire	Mesures	Statut
Fuite de données via messagerie	Renforcement de l'anti-phishing, prévention	A mettre en place
Accès non sécurisé aux postes	Déploiement systématique du verrouillage auto et charte de bon usage	En place
Partage de documents sensibles	Centralisation via solution sécurisée Drive entreprise	En place
Risques liés aux fournisseurs numériques	Audit des clauses de sécurité / RGPD des contrats IT, demande d'attestation conformité	A mettre en place
Systèmes en points de vente	Vérification des terminaux, mise à jour sécurité, mots de passe pour les vendeurs	En place

· Toute transaction réalisée depuis un pays différent de celui associé à la carte de paiement utilisée est bloquée.
· Tout virement bancaire émis ou reçu nécessitant une double vérification, incluant un contre-appel téléphonique auprès du contact référencé pour validation.

C) Actions de protection des données mises en place

Dans le cadre de sa politique de protection des données personnelles, Sanipod a déployé une **infrastructure de sécurité réseau professionnelle**, incluant l'installation d'un pare-feu physique de type UTM (Unified Threat Management).

Depuis août 2023, une appliance de sécurité SN160, configurée avec deux zones réseau distinctes, a été mise en place par l'intégrateur Digital-Liance. Cette solution permet notamment :
· Le filtrage des connexions entrantes et sortantes vers les systèmes contenant des données sensibles (clients, fournisseurs, etc.) ;
· La limitation des accès aux seuls postes internes habilités, grâce à une segmentation réseau ;
· La journalisation des connexions et tentatives d'accès, en conformité avec les recommandations de la CNIL ;
· Une protection active contre les intrusions, malwares et tentatives de fuite de données, assurée par un pack de sécurité UTM.

Parallèlement, l'entreprise utilise la solution **Dropbox Business** pour le stockage et le partage sécurisé des fichiers professionnels. L'accès aux répertoires est strictement encadré selon les responsabilités de chaque utilisateur :
· Chaque collaborateur n'a accès qu'aux dossiers nécessaires à l'exercice de ses fonctions ;· Un audit régulier des droits d'accès est mené pour garantir le respect des règles de confidentialité internes.

L'ensemble de ces dispositifs, complétés par un **hébergement sécurisé** en France ou dans l'Union européenne (via OVH), ce qui constitue une mesure technique et organisationnelle solide, conforme à l'article 32 du RGPD, visant à assurer l'intégrité, la confidentialité et la disponibilité des données personnelles.

VIII – REPORTING SUR L'ÉTHIQUE DES AFFAIRES

Indicateur	2023	2024	2025
Nombre d'incidents signalés via la procédure d'alerte	0	0	0
Nombre d'incidents confirmés liés à des faits de corruption	0	0	0
Nombre d'incidents confirmés relatifs à la sécurité de l'information	0	0	0

Au cours des dernières années, **aucun incident n'a été signalé via les procédures d'alerte (voir Annexes) et aucun cas avéré de corruption, de fraude, de conflit d'intérêts ou d'atteinte à la sécurité de l'information** n'a été constaté. Ces résultats reflètent la robustesse de notre politique d'éthique des affaires, fondée sur la transparence, la prévention active des risques et l'implication de toutes les parties prenantes.

Sanipod souhaite maintenir ce niveau d'exigence et conserver un score de **zéro incident**, en poursuivant ses efforts de vigilance, de formation et de sensibilisation.

Dans cette optique, un programme de **formation à l'éthique des affaires** va être étudié dès 2026, avec pour objectif de **former 100 % des collaborateurs exposés** à des fonctions sensibles (achats, finance, RH, direction). Cette démarche vise à renforcer la culture de l'intégrité au sein de l'entreprise et à garantir une maîtrise partagée des risques éthiques.

ANNEXE 1 – PROCÉDURE D'APPROBATION SPÉCIFIQUE POUR LES TRANSACTIONS SENSIBLES

Ce dispositif vise à encadrer l'**approbation des transactions sensibles**, c'est-à-dire des opérations comportant un risque accru de corruption, de fraude, ou de conflit d'intérêts. Il est mis en œuvre conformément à la loi Sapin II et intégré à notre programme de prévention des risques éthiques.

A) Définition des transactions sensibles

Sont considérées comme transactions sensibles chez Sanipod :

- Toute relation commerciale nouvelle à l'international ;
- Toute nouvelle contractualisation ou agrégation d'un fournisseur ou prestataire stratégique ;
- Toute modification contractuelle majeure avec un fournisseur existant ;
- Toute dépense de mécénat, sponsoring ou cadeau d'un montant unitaire supérieur à 300 € TTC ;
- Tout encaissement en provenance d'un pays classé à risque élevé, figurant sur une liste noire ou grise (GAFI) ;
- Toute transaction réalisée depuis un pays différent de celui associé à la carte de paiement utilisée ;
- Tout virement bancaire émis ou reçu nécessitant une double vérification, incluant un contre-appel téléphonique auprès du contact référencé pour validation.

B) Etapes clés

1. Identification de la transaction sensible par le collaborateur en charge ;
2. Contact du référent éthique à l'adresse ***olivier.richard@hardrige.com*** décrivant : les parties impliquées, l'objet, le montant et les risques identifiés.
3. Validation par la Direction avant la transaction

ANNEXE 2 – PROCÉDURE D'ALERTE À DISPOSITION DES PARTIES PRENANTES AFIN DE SIGNALER TOUTE FORME DE CORRUPTION

A) Garantie de confidentialité

Tous les signalements reçus dans le cadre de cette procédure sont traités avec la plus stricte confidentialité, dans le respect des dispositions du Code du travail et de la loi Sapin II.

Les éléments suivants sont protégés :

- L'identité du lanceur d'alerte (sauf accord exprès de sa part) ;
- L'identité de la ou des personnes visées par l'alerte ;
- Les faits objets du signalement.

Les dossiers sont conservés de manière sécurisée, avec un accès restreint aux seules personnes chargées du traitement.

B) Garantie d'absence de représailles

Aucune mesure de représailles, discrimination ou sanction ne peut être prise à l'encontre d'un lanceur d'alerte qui a agi de bonne foi, même si les faits s'avèrent infondés.
Toute tentative d'intimidation ou de sanction abusive à l'encontre d'un lanceur d'alerte fera l'objet de mesures disciplinaires.
L'entreprise se réserve le droit d'engager des actions en justice en cas de signalement abusif, malveillant ou diffamatoire.

C) Procédure de signalement

Toute personne ayant un lien professionnel avec Sanipod peut effectuer un signalement dans le cadre de cette procédure. Cela inclut l'ensemble des collaborateurs ainsi que les fournisseurs, sous-traitants, distributeurs, clients ou partenaires externes.

Les faits pouvant faire l'objet d'un signalement sont notamment :

- Toute tentative ou acte avéré de corruption, tels que des avantages indus, pots-de-vin ou commissions dissimulées ;
- Un conflit d'intérêts non déclaré, notamment lorsqu'il influence une décision d'achat ou de partenariat ;
- Des cadeaux ou invitations dépassant les usages professionnels raisonnables ou non conformes à la politique interne ;
- Le recours à un intermédiaire dont le rôle ou la rémunération semble suspect ou injustifié.

Le signalement peut être réalisé de manière confidentielle et sans représailles en envoyant un mail au référent éthique : ***olivier.richard@hardrige.com***.

ANNEXE 3 – PROCÉDURE D'ALERTE À DISPOSITION DES PARTIES PRENANTES AFIN DE SIGNALER LES PROBLÈMES EN MATIÈRE DE SÉCURITÉ DE L'INFORMATION

A) Garantie de confidentialité

Tous les signalements reçus relatifs à la sécurité de l'information sont traités dans le respect absolu de la confidentialité, conformément au Code du travail, à la loi Sapin II et au Règlement Général sur la Protection des Données (RGPD).

Sont notamment protégés :

- L'identité du lanceur d'alerte (sauf s'il autorise expressément sa divulgation) ;
- L'identité des personnes visées par l'alerte ;
- Les faits et données techniques signalées.

Les dossiers sont conservés de manière sécurisée et accès limité aux seules personnes habilitées au sein de l'entreprise, dans le cadre du traitement de l'alerte.

B) Garantie d'absence de représailles

Aucune mesure de représailles, sanction ou discrimination ne sera engagée à l'encontre d'une personne ayant émis un signalement de bonne foi, même si les faits rapportés ne sont pas avérés.
Les intimidations, pressions ou mesures abusives à l'égard du lanceur d'alerte feront l'objet de mesures disciplinaires internes.
À l'inverse, tout signalement volontairement mensonger ou malveillant pourra donner lieu à des sanctions et le cas échéant, à des poursuites judiciaires.

C) Procédure de signalement

Toute personne ayant un lien professionnel avec Sanipod peut effectuer un signalement dans le cadre de cette procédure. Cela inclut l'ensemble des collaborateurs ainsi que les fournisseurs, sous-traitants, distributeurs, clients ou partenaires externes.

Les signalements peuvent concerner :

- Une faille de sécurité ou une vulnérabilité constatée dans les outils de l'entreprise ;
- Un accès non autorisé à un système ou fichier confidentiel ;
- La perte ou divulgation accidentelle de données sensibles ;
- Un comportement anormal d'un système, suspecté d'être lié à une attaque (phishing, ransomware, etc.) ;
- Toute pratique contraire aux règles de sécurité informatique internes.

Le signalement peut être réalisé de manière confidentielle en envoyant un mail au référent éthique : ***olivier.richard@hardrige.com***.

ANNEXE 4- PLAN DE RÉPONSE AUX INCIDENTS POUR GÉRER LES ATTEINTES AUX INFORMATIONS CONFIDENTIELLES

A) Objectif du dispositif

Ce plan vise à encadrer la réaction de l'entreprise face à une atteinte à la sécurité de l'information, notamment en cas de :

- Fuite, perte ou vol de données personnelles ou confidentielles ;
- Accès non autorisé aux systèmes d'information ;
- Infection par un logiciel malveillant (ransomware, virus, etc.) ;
- Erreur humaine entraînant une divulgation accidentelle de données.

L'objectif est de limiter l'impact de l'incident, d'en réduire la portée, de rassurer les parties concernées et d'éviter toute récurrence.

B) Garantie d'absence de représailles

Toute personne (salarié, prestataire, responsable de site ou de boutique) peut détecter un incident ou une anomalie liée à la sécurité de l'information.
Les signaux d'alerte peuvent inclure :

- Un comportement anormal du système (ralentissement, blocage, message suspect) ;
- Une notification d'un partenaire ou client concernant des données mal adressées ;
- Une tentative de phishing, d'usurpation ou un accès injustifié à un compte.

Toute suspicion doit être signalée sans délai au service informatique ou directement à l'adresse suivante : ***olivier.richard@hardrige.com***.

C) Procédure en cas d'incident

Dès la détection :

- Isolez le poste ou l'équipement concerné (déconnexion réseau, arrêt du poste si nécessaire) ;
- Prévenez immédiatement le référent interne ;
- Ne tentez pas de corriger ou d'effacer les traces de l'incident vous-même.

L'équipe en charge effectue une première analyse technique rapide pour :

- Identifier l'origine et la nature de l'incident ;
- Évaluer les données et systèmes affectés ;
- Contenir la propagation ou l'impact immédiat.

C) Rétablissement et mesures correctives

Une fois l'incident contenu :

- Rétablissement du service via sauvegarde, mise à jour de sécurité, changement de mot de passe ou remplacement du matériel ;
- Mise en œuvre de mesures correctives : renforcement des contrôles, ajustement de procédure, restriction d'accès ;
- Sensibilisation ciblée auprès des personnes ou équipes concernées si l'origine est humaine.