Politique de Prévention et de Lutte contre la Fraude

Prévention, détection, enquête et sanctions

Entreprise	EBI
Version	1.0
Date d'effet	Décembre 2025
Préparé par	Mohamed Kébé, Responsable du personnel
Approuvé par	Direction générale
Responsable	Direction générale et Ressources Humaines

Cette politique vise à prévenir, détecter et sanctionner toute forme de fraude financière, opérationnelle, informatique, technique ou liée aux achats.

1. Objectif

- Prévenir, détecter et sanctionner toute forme de fraude.
- Protéger les actifs financiers, matériels et immatériels d'EBI.
- Assurer l'intégrité des opérations et renforcer la confiance des clients, partenaires et institutions.

2. Champ d'application

- Employés, formateurs, consultants, techniciens, sous-traitants, partenaires et toute personne agissant pour le compte d'EBI.

3. Définition

La fraude désigne tout acte intentionnel visant à tromper dans le but d'obtenir un avantage indu.

4. Types de fraude couverts

- Fraude financière : détournement de fonds, fausse facturation, double paiement, manipulation des comptes.
- Fraude opérationnelle : prestations non réalisées, falsification de rapports techniques ou de présences en formation.
- Fraude liée aux achats : ententes avec fournisseurs, surfacturation, fournisseurs fictifs.
- Fraude IT et cybersécurité : accès non autorisé, vol de données, manipulation des systèmes, logiciels frauduleux.
- Fraude terrain : faux rapports de conformité incendie, fausses interventions en sauvetage minier, certificats délivrés sans formation réelle, matériel réseau facturé mais non installé.

5. Principes fondamentaux

- Tolérance zéro : toute fraude est interdite, quel que soit son montant.
- Responsabilité individuelle : chaque collaborateur est responsable de ses actes.
- Transparence : toutes les opérations doivent être traçables et justifiées.

6. Mesures de prévention

- Séparation des tâches : une seule personne ne doit pas contrôler toute une opération.
- Contrôles internes : vérification des factures, validation des prestations, suivi des stocks et équipements.
- Vérification des partenaires : identification des fournisseurs, analyse des antécédents et contrats formalisés.
- Gestion IT sécurisée : accès contrôlés, sauvegarde des données et traçabilité des actions.

7. Détection et signalement

- Signaux d'alerte : incohérences dans les factures, absence de justificatifs, pression pour valider rapidement, comportement suspect, écarts entre terrain et rapports.
- Tout employé doit signaler une fraude, une tentative ou une suspicion.
- Canaux : Ressources Humaines, Direction générale, canal confidentiel ou compliance@ebi-gn.com.
- Aucune représaille contre les lanceurs d'alerte de bonne foi.

8. Enquête

- Toute suspicion donne lieu à une enquête interne, collecte de preuves et audition des personnes concernées.
- Si nécessaire, EBI peut recourir à un expert externe.

9. Sanctions

- Selon la gravité : avertissement, suspension, licenciement ou poursuites judiciaires.

10. Formation et responsabilités

- EBI forme régulièrement ses équipes au moins une fois par an et dès la prise de fonction des nouvelles recrues.
- La Direction met en place les contrôles et donne l'exemple ; les managers surveillent les activités ; les employés respectent les règles et signalent les risques.

11. Conservation et engagement

- Contrats, factures, rapports et données IT sont conservés pendant une durée minimale recommandée de cinq ans.
- EBI maintient un environnement de travail intègre, protège ses ressources et collabore avec les autorités en cas de fraude.

Approbation

Nom	Robert TOUNKARA
Fonction	Directeur général
Organisation	EBI