POLITIQUE DE SECURITE ET SURETE DE COSAWOH

Version révisée 2025

Politique de sécurité et sûreté de COSAWOH

1. Contexte et justification

COSAWOH intervient dans des environnements où la sécurité du personnel, des bénéficiaires et des actifs peut être menacée par des facteurs naturels, politiques, sanitaires ou criminels.

Cette politique formalise les principes et procédures à suivre pour prévenir les incidents, protéger les équipes sur le terrain et assurer la continuité des opérations humanitaires.

2. Objectifs

1. Protéger la vie et l'intégrité physique du personnel, des volontaires et des bénéficiaires.
2. Garantir la sécurité des infrastructures, des biens et des données de l'ONG.
3. Prévenir, identifier et gérer efficacement les incidents de sécurité et sûreté.
4. Assurer la continuité des activités critiques en cas de crise ou d'urgence.
5. Renforcer la résilience organisationnelle par la formation, le suivi et l'évolution permanente des procédures.

3. Principes directeurs

- Prévention : anticiper et réduire la probabilité d'incidents grâce à l'évaluation systématique des risques.
- Proportionnalité : adapter les mesures de sécurité à la gravité des menaces et aux ressources disponibles.
- Responsabilité partagée : impliquer chaque collaborateur dans la gestion de sa propre sécurité et de celle de ses pairs.
- Transparence : communication claire des protocoles, des alertes et des retours d'expérience.
- Respect des droits humains : veiller à ce que les mesures de sûreté n'enfreignent pas la dignité ou la liberté des individus.
- Collaboration : coordonner les actions de sécurité avec les autorités locales, les autres ONG et les communautés.

4. Champ d'application

Cette politique s'applique à :

- Tout le personnel permanent, contractuel, consultant, volontaire et stagiaire.
- Tous les sites administratifs et projectifs de COSAWOH (sièges, bureaux régionaux, entrepôts, centres de distribution).
- Tous déplacements, missions et événements organisés par l'ONG.
- La gestion des actifs physiques (véhicules, équipements) et numériques (systèmes informatiques, bases de données).

5. Gouvernance et responsabilités

Acteur	Responsabilités clés
Conseil d'Administration	Validation de la politique, arbitrage en cas de crise majeure
Directeur Exécutif	Supervision de la mise en œuvre globale, décision sur l'activation des plans d'urgence
Responsable Sécurité & Sûreté	Élaboration, mise à jour et coordination de la politique, animation des comités de sécurité, suivi des incidents
Chefs de projet	Réalisation des évaluations de risques terrain, respect des protocoles sur site, reporting des incidents
Managers locaux	Briefings réguliers, contrôle de l'application des mesures (accès, gardiennage, communication), remontée des alertes
Tous les collaborateurs	Connaissance et respect des procédures, participation aux formations, signalement immédiat de toute situation à risque

6. Gestion des risques de sécurité

6.1 Identification et évaluation des risques

- Cartographie des menaces principales (conflit armé, vol, agression, catastrophe naturelle, cyberattaque).
- Analyse de l'exposition selon la zone, la saison, l'activité (tableau ci-dessous).

Zone / Activité	Risque principal	Probabilité	Impact potentiel	Niveau de risque
Siège urbain	Vol / intrusion	Moyen	Moyen	Moyen
Mission en zone rurale	Agression armée	Faible	Élevé	Moyen-Élevé
Distribution de vivres	Attroupement / bousculade	Élevé	Élevé	Élevé
Système d'information	Phishing / ransomware	Moyen	Élevé	Moyen-Élevé

6.2 Plan de mitigation

- Renforcement des accès (grilles, contrôle biométrique, gardiennage).
- Protocoles de convoyage sécurisés pour les actifs et le personnel.
- Procedures IT : pare-feu, antivirus, sauvegardes chiffrées, gestion des accès.
- Coordination avec la sécurité locale (police, armée, comités communautaires).
- Mise en place de kits d'urgence (trousse de premiers secours, radio, lampes torches, vivres de survie).

`7. Sécurité du personnel

7.1 Briefing avant mission

- Session pré-départ pour exposer les menaces spécifiques, itinéraires sécurisés et contacts d'urgence.
- Distribution de la « fiche de mission sécurité » précisant : coordonnées des référents, points de rendez-vous, fréquences de communication.

7.2 Protocoles de déplacement

- Validation préalable de tout déplacement par le Responsable Sécurité & Sûreté.
- Utilisation systématique de convoys ou de chauffeurs formés aux règles de comportement en zone à risque.
- Itinéraire alternatif et plan de replis en cas d'imprévu.

7.3 Communication et suivi

- Check-in quotidien via SMS, radio VHF ou application mobile sécurisée.
- Système SOS embarqué dans les véhicules.
- Ligne d'alerte 24/7 gérée par un référent dédié.

8. Sécurité des sites et des infrastructures

- Contrôle d'accès strict : badges, liste des visiteurs, registre de sécurité.
- Rondes régulières par un agent habilité, vérification des points sensibles (issues de secours, clôtures).
- Systèmes d'alarme et caméras de surveillance connectés à un centre de monitoring local.
- Stockage sécurisé des matériels sensibles (kits médicaux, documents confidentiels) dans des coffres ou armoires verrouillées.

9. Sécurité des équipements et des actifs

- Inventaire annuel et vérification trimestrielle des véhicules, générateurs, équipements informatiques.
- Plaques d'immatriculation non-identifiables en zone à risque, marquages discrets hors mission.
- Suivi GPS des véhicules avec géo-clôture et alertes en cas de déviation non autorisée.
- Politique d'obsolescence : retrait sécurisé et destruction des appareils hors d'usage contenant des données sensibles.

10. Continuité des activités et plans d'urgence

10.1 Plan de réponse aux incidents

1. Activation de l'équipe d'intervention (security incident response team).
2. Évaluation rapide de la situation et mise en sécurité des personnes.
3. Coordination avec les secours locaux et les bailleurs.
4. Communication interne et externe (porte-parole désigné).

10.2 Plan de continuité d'activité (PCA)

- Identification des fonctions critiques (financement, approvisionnement, communication).
- Scénarios de rupture majeure (inondation du siège, cyberattaque, évacuation d'urgence).
- Solutions de repli : bureaux satellites, accès cloud sécurisé, redondance des liaisons Internet.

11. Formation et renforcement des capacités

- Modules obligatoires pour tout nouveau collaborateur : sensibilisation à la sécurité, premiers secours, conduite en situation d'urgence.
- Exercices semestriels de simulation d'incident (évacuation, prise d'otage, cyberattaque).
- Ateliers avancés pour responsables de site : gestion de crise, négociation en cas de kidnapping.
- Evaluation annuelle des connaissances et maintien des certifications (CIC, NEBOSH ou équivalent).

12. Gestion des incidents et reporting

- Formulaire standardisé d'enregistrement des incidents (date, lieu, nature, témoins, dommages).
- Délai maximal de 24 heures pour toute déclaration d'incident majeur au Responsable Sécurité & Sûreté.
- Retour d'expérience (REX) organisé après chaque incident pour identifier les leçons apprises et ajuster les procédures.

13. Audit, suivi et amélioration continue

- Audit interne annuel mené par le comité de sécurité en lien avec le service Compliance.
- Indicateurs clés : nombre d'incidents, temps de réponse moyen, taux de participation aux exercices.
- Revue semestrielle de la politique et mise à jour en fonction des retours terrain et de l'évolution du contexte.

14. Collaboration et partenariats

- Coordination avec les autorités locales (police, services de santé, défense civile).
- Partenariat avec d'autres ONG pour la mutualisation des informations de sécurité.
- Participation aux groupes de sécurité sectoriels et échanges d'alertes précoces (SITREP).

Annexes

- Annexe 1 : Fiche de mission sécurité
- Annexe 2 : Formulaire d'enregistrement d'incident
- Annexe 3 : Matrice des risques détaillées par zone
- Annexe 4 : Procédures d'évacuation et checklist du PCA
- Annexe 5 : Guide de négociation en cas de prise d'otage

Cette politique garantit que tous les acteurs de COSAWOH disposent d'un cadre clair et structuré pour anticiper, prévenir et réagir efficacement face aux menaces, tout en assurant la sécurité et la continuité de nos missions.