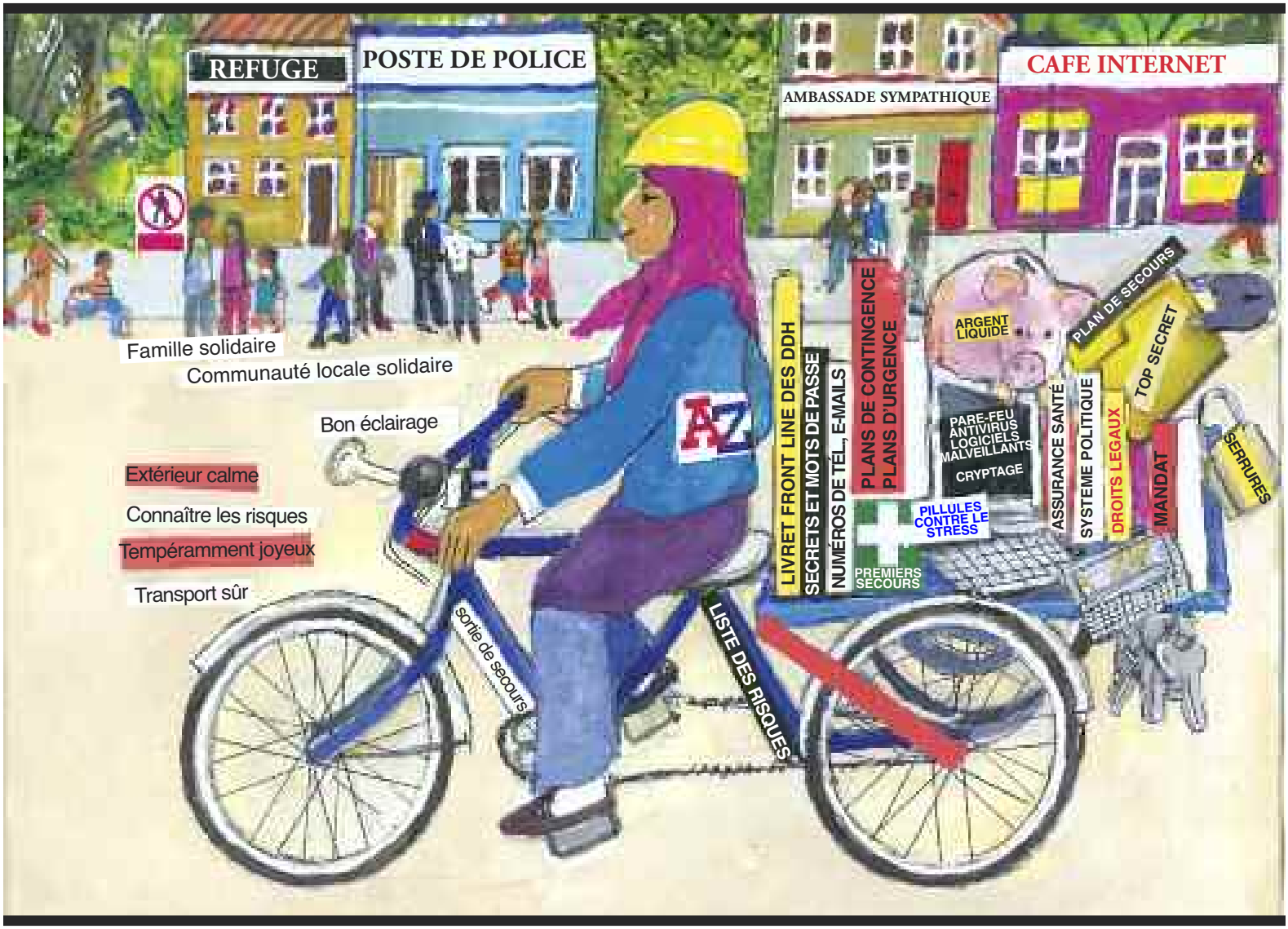
MANUEL DE SÉCURITÉ :

MESURES PRATIQUES POUR LES DÉFENSEURS DES DROITS HUMAINS EN DANGER



FRONT LINE DEFENDERS

ANNEXE 5

Liste de contrôle : La sécurité au bureau

Cette liste de contrôle n'est pas un plan de sécurité. Votre propre contexte est le facteur clé déterminant. Considérez les risques et les menaces auxquels vous êtes exposé, ainsi que toutes vos vulnérabilités.

1. Contacts en cas d'urgence :
   - Y a-t-il une liste à jour et à portée de main des numéros de téléphones et adresses des autres ONG locales, des hôpitaux d'urgence, de la police, des pompiers et des ambulances ?

2. Barrières techniques et matérielles (externes, internes et à l'intérieur)
   - Vérifiez l'état et le fonctionnement des portails/clôtures externes, des portes d'entrée du bâtiment, des fenêtres, des murs et du toit
   - Vérifiez l'état et le bon fonctionnement de l'éclairage à l'extérieur, des alarmes, des caméras ou des interphones vidéo
   - Vérifiez les procédures relatives aux clés ; vérifiez que les clés soient bien gardées et étiquetées selon un code garantissant leur sécurité ; vérifiez l'attribution des responsabilités du contrôle des clés et de leurs doubles ; vérifiez que les clés et les doubles fonctionnent. Veillez à ce que les serrures soient changées en cas de perte ou de vol des clés, et qu'on ait fait un rapport sur la perte ou le vol.
   - Avez-vous une pièce plus "sécurisée" ?
   - Est-ce que l'enseigne indiquant votre bureau peut être retirée en période de menaces, afin de réduire la probabilité d'une attaque ?

3. Le personnel de l'organisation :
   - Recrutez-vous uniquement du personnel de confiance, y compris les gardes, et prenez-vous leurs références ?
   - Est-ce que tout le personnel est formé aux plans de sécurité qui peuvent les concerner ?
   - Avez-vous un plan si votre bureau est perquisitionné par les autorités ou d'autres groupes ?
   - Avez-vous une politique "besoin de savoir" concernant le travail le plus sensible ?
   - Maintenez-vous une bonne communication avec tous les employés, en particulier si vous savez qu'ils ont des problèmes financiers ou subissent d'autres pressions ? (les employés mécontents peuvent devenir de dangereux ennemis)
   - Lorsque quelqu'un quitte l'organisation, changez-vous les mesures de sécurité, les mots de passe, les clés ?

4. Les procédures d'admission et le "filtrage" des visiteurs
   - Existe-il des procédures d'admission en vigueur pour chaque type de visiteur ? Est-ce que tout le personnel les connaît et les applique ?
   - Demandez aux membres du personnel responsables des procédures d'admission si celles-ci fonctionnent correctement et dans le cas contraire, quelles améliorations sont nécessaires.
   - Les employés savent-ils quoi faire si un colis inattendu est livré ? (par exemple, l'isoler, ne pas l'ouvrir, appeler les autorités)
   - Ecrivez-vous les noms des visiteurs (y compris ceux qui participent à des réunions dans votre bureau) ? Si oui, ces informations sont-elle sensibles et comment les protégez-vous ? (Par exemple par des codes ou des fichiers cryptés)

5. Sécurité de l'information (voir aussi l'annexe 14, Sécurité des ordinateurs et des téléphones)
   - Faîtes-vous des sauvegardes régulières et conservez-vous ces sauvegardes dans un lieu sûr hors du bureau ?
   - Est-ce que les employés savent qu'il ne faut pas laisser des informations sensibles sur leur bureau ?
   - Avez-vous un système sécurisé pour enregistrer les informations confidentielles, par exemple sur les clients ou les témoins ?
   - Donnez-vous des noms sécurisés à vos dossiers (papiers ou électroniques), afin qu'ils ne soient pas immédiatement identifiables

6. Sécurité en cas d'accident
   - Vérifiez l'état des extincteurs, des valves/tuyaux à gaz et des robinets d'eau, des prises électriques et des câbles, des générateurs d'électricité (s'ils existent)

7. Responsabilité et formation
   - A-t-on désigné un(e) responsable de la sécurité ? Est-ce efficace ?