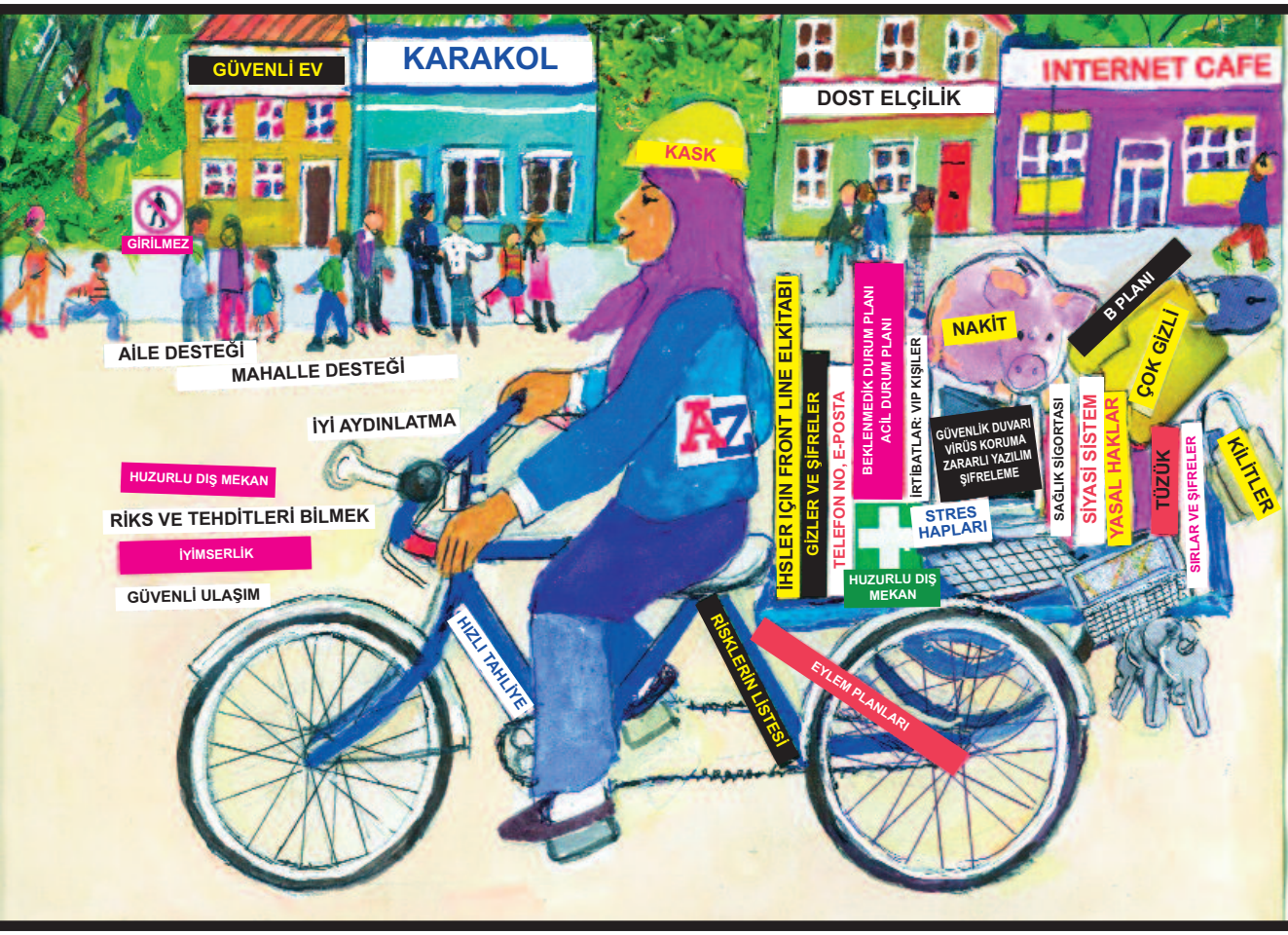
GÜVENLİK EL KİTABI:

RİSK ALTINDAKİ İNSAN HAKLARI SAVUNUCULARI İÇİN PRATİK ADIMLAR



FRONT LINE DEFENDERS

EK 5

Kontrol listesi: Ofis Güvenliği

Bu kontrol listesi güvenlik için bir şablon olması amacıyla hazırlanmamıştır. Temel belirleyici faktör size özgü şartlardır (bağlam). Bu listeyi kişiselleştirmek için karşınızdaki riskleri ve tehditleri ve zayıf yönlerinizi dikkate alın.

1. Acil Durum İrtibatları
- Elinizin altında, diğer yerel STK'ların, hastanelerin ve acil servislerin, polis, itfaiye ve ambulans telefonlarının olduğu güncellenmiş bir liste var mı?

2. Teknik ve fiziki sınırlar (harici, dahili ve iç mekan)
- Dış kapıların / parmaklıkların, bina giriş kapılarının, pencere, duvar ve çatının durumunu ve çalışır durumda olup olmadıklarını kontrol edin
- Harici ışıklandırmanın, alarmların, kamera veya görüntülü diyafonun durumunu ve çalışıp çalışmadığını kontrol edin
- Anahtarlarla ilgili prosedürü kontrol edin - anahtarlar güvenli ve şifreli bir biçimde etiketlenmiş mi, anahtar kontrolünden, kopyalanmasından ve kopyaların çalışıp çalışmadığını kontrol etmekten sorumlu bir kişi tayin edin. Anahtarların kaybolması veya çalınması durumunda kilitlerin değiştirildiğinden emin olun ve bu gibi olayların kaydını tutun
- Özel bir 'güvenli' oda var mı? (panik odası)
- Kurumun isminin olduğu tabela/plaka, tehditin arttığı durumlarda saldırılara karşı tedbiri artırmak için kolayca sökülebilir mi

3. Ofis personeli
- Korumalar/bekçiler dahil personel alımında yalnızca güvenilir kişiler mi işe alınıyor ve verilen referanslar kontrol ediliyor mu?
- Tüm personel ilgili güvenlik planları konusunda eğitiliyor mu?
- Ofisin yetkililer veya farklı gruplarca basılması ihtimaline karşı bir planınız var mı?
- En hassas işler konusunda 'bilmen kadarını bil' (need-to-know) politikanız var mı?
- Tüm çalışanlarla iyi bir diyalogunuz var mı, özellikle de finansal sorunları veya başka sorunlar yüzünden baskı altında hissettikleri durumlarda sizinle konuşabiliyorlar mı? (canı sıkkın çalışan tehlikeli bir düşman olabilir)
- Birisi kurumdan ayrıldığında güvenlik tedbirlerini ve ilgili anahtarları değiştiriyor musunuz?

4. Ziyaret kabul prosedürleri ve 'filtreleri'
- Tüm ziyaretçilere uygulanan bir kabul prosedürünüz var mı? Tüm ekip bundan haberdar mı?
- Kabul prosedürlerini uygulayan personele işlemin gerektiği gibi işleyip işlemediğini ve geliştirilmesi/değişmesi gereken bir şeylerin olup olmadığını sorun
- Beklenmeyen bir paket/posta geldiğinde ekip ne yapması gerektiğini biliyor mu? (izole etmek, açmamak, yetkilileri çağırmak gibi)
- Ziyaretçilerin isimleri kaydediliyor mu (ofisinizdeki bir toplantıya katılmak için gelenler de dahil)? Evetse, bu kayıtlar hassas bilgi kapsamında mı ve nasıl korunuyor? (örneğin kodlar veya şifrelenmiş dosyalar)

5. Bilgi güvenliği (ayrıca bkz. Ek 14, Bilgisayar ve Telefon Güvenliği)
- Düzenli olarak yedekleme yapıyor musunuz; yedekleri ofis dışında, güvenli bir yerde mi saklıyorsunuz?
- Çalışanlar masalarında hassas bilgi bırakmamaları gerektiğini biliyor mu?
- Mahrem bilgileri (örneğin başvuranlar veya tanıklar hakkında) kaydetmek için güvenli bir sisteminiz var mı?
- Hassas (fiziksel ve elektronik) dosyalarınıza ilk bakışta ne oldukları anlaşılmasın diye güvenli isimler veriyor musunuz?

6. Kaza durumları için güvenlik
- Yangın söndürücülerini, gaz vanalarını ve borularını, muslukları, elektrik prizlerini ve kablolarını ve jeneratörlerin durumunu kontrol edin.

7. Sorumluluk ve eğitim
- Ofis güvenliği için sorumlular belirlendi mi? Etkin biçimde çalışıyor mu?
- Bir ofis güvenlik eğitim programı var mı? Bu listede yer alan tüm konuları kapsıyor mu? Yeni ekibin tamamı eğitim aldı mı? Eğitim etkili mi?