BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

POSTA SEKTÖRÜNE YÖNELİK GÜVENLİK STANDARTLARI

İÇİNDEKİLER

Modül 1:

UPU Kanun ve Yönetmelikleri 3

Modül 2:

S58-Posta Güvenliği Standartları- Genel Güvenlik Önlemleri 6

Modül 3:

S59- Posta Güvenlik Standartları- Borsa ve Uluslararası Havayolu Ofisi 25

Modül 4:

Postadaki Tehlikeli Mallar 34

Modül 5:

Yasaklı Malların Postalanmasının Kötüye Kullanımı - Uyuşturucu Trafiği Hedefleri 46

Modül 6:

Dâhili ve Harici Posta Hırsızlığı - Dâhili Posta Hırsızlığı 69

Modül 7:

Gelir Koruma 2015 81

Modül 1: UPU Kanun ve Yönetmelikleri

Modül sonunda şu hususlar açıklanıyor olacak:

- Dünya Posta Birliği'nin (UPU) temel yapısı
- Önemli kural ve düzenlemeleri ve bunların nerede bulunacağını
- Posta Güvenlik Grubu'nun (PGG) UPU içerisinde nasıl yer aldığını
- UPU'nin diğer Uluslararası Kuruluşlarla nasıl ve neden etkileşimde olduğunu

UPU dört birimden oluşur:

- Üye ülkelerce tanınan belirlenmiş işletmeciler, UPU Anlaşmasına ve onun Detaylı Yönetmeliklerine tabidir.
- UPU, devletlerarası konuları anlaşma seviyesinde ele alır.
- Yalnızca UPU temel yönetim birimi olan Kongre, UPU Anlaşması'nda değişikliğe gidebilir.

2013-2016 Doha Posta Stratejisi

25. Evrensel Posta Kongresi 24 Eylül 15 Ekim 2012 tarihleri arasında Doha, Katar'da gerçekleştirilmiştir.

Doha Posta Stratejisi 2016 yılına kadar aşağıdaki dört hedefe ulaşmayı amaç olarak benimsemiştir:

1. Uluslararası posta ağlarının birlikte çalışabilirliğini artırmak

2. Posta sektörüne ilişkin hem uzmanlık hem de teknik bilgi sağlamak
3. Yenilikçi ürün ve hizmetleri teşvik etmek
4. Posta sektörünün sürdürülebilir gelişimini desteklemek

Program 1.2.: Posta birliği, bütünlüğü ve güvenliğini artırmak ve gümrük süreçlerini kolaylaştırmak.

- Posta güvenliği, genel olarak Doha Posta Stratejisi'nin birincil unsurudur.

Doha Kongresi, Anlaşma Maddesi 9'da aşağıdaki değişikliğe gitmiştir:

Üye ülkeler ve onların yetkilendirilmiş işletmecileri, UPU güvenlik standartlarında belirlenen güvenlik gerekliliklerini yerine getirmekle yükümlüdür. Bununla birlikte bu işletmeciler kamunun güvenini pekiştirmek ve sürdürmek amacıyla, posta sürecinin her kademesinde proaktif/ön alıcı güvenlik stratejilerini benimsemeli ve uygulamalıdır.

Doha Kongresi, Anlaşma Maddesi 9'da aşağıdaki değişikliğe gitmiştir:

Bu strateji, özellikle, UPU teknik mesajlaşma standartlarına uygun olarak Posta İşlemleri Konseyi ve Yönetim Kurulu tarafından kabul edilen uygulama hükümlerinde (posta kalemlerinin türleri ve kıstasları da dahil) tanımlanan posta kalemlerinde elektronik avans veri sağlama gerekliliklerivle uyumlu olma ilkesini içeriyor olmalıdır.

Bu strateji aynı zamanda, üye ülkeler ve bunların belirlenmiş işletmecileri arasında postaların güvenli ve emin bir şekilde taşınması ve aktarımının sürdürülmesi konusunda bilgi aktarımını da kapsıyor olmalıdır.

Posta İşlemleri Kurul Komitesi 1 – Tedarik Zinciri Entegrasyonu

POSTA GÜVENLİĞİ GRUBU	NAKLİYE GRUBU	İŞLETİM VE MUHASEBE GRUBU
GÜMRÜK GRUBU	STANDARTLAR KURULU	ADRESLEME

Posta İşlemleri Konsey Komitesi 1- Tedarik Zinciri Entegrasyonu

- 20. Washington Kongresi'nde oluşturulmuştur.
- UPU merkezi bürosunda yılda iki kez İsviçre'nin Bern kentinde toplanmaktadır.
- Posta işletmecileri arasındaki en iyi uygulamalar ve güvenlik standartlarının uygulanması ve geliştirilmesine yönelik hizmet araçlarını kapsar.
- 1. Komite (K1) Tedarik Zinciri Entegrasyonu aracılığıyla Posta İşlemleri Konseyi raporlarını kapsar.

Posta Güvenliği Grubu (PGG) Misyon ve Öncelikleri

Bütün dünyada posta güvenliğini sağlamak, tüm UPU üye ülkelerinde posta güvenlik hizmetlerinin oluşturulmasını teşvik etmek ve ilerletmek, uluslararası kuruluşlarla iletişim kurmak ve işbirliği yapmak

- Postada tehlikeli malların taşınması nedeniyle oluşabilecek yaralanmaların önlenmesi
- Şubelere zimmetlenen postaların kaybının veya çalınmasının önlenmesi
- Posta yoluyla gelir veya mal kaybının önlenmesi
- Kullanıcıların posta işletmecilerine olan güven kaybının engellenmesi

PGG'nin Uluslararası Organizasyonlarla İlişkileri

- Uluslararası postalar farklı yöntemlerle taşınır
- Uluslararası postaların birincil taşıma yöntemi hava yoludur
- Uluslararası posta, dünya çapında gümrük idaresine giriş ve çıkış yapar.
- PGG, posta operasyonları üzerinde etkisi olabilecek kanun ve yönetmelikler oluşturan uluslararası kuruluşlarla gerçekleştirilen toplantılara ve çalışma gruplarına katılmaktadır

Kuralları ve Yönetmelikleri Posta İşlemlerini Etkileyen Uluslararası Kuruluşlara Örnekler

- Uluslararası Sivil Havacılık Örgütü (ICAO)
- Uluslararası Hava Taşımacılığı Birliği (IATA)
- Dünya Gümrük Örgütü (WCO)
- Birleşmiş Milletler Uyuşturucu ve Suç Ofisi (UNDOC)
- Birleşmiş Milletler Ekonomik ve Sosyal Konsey Uzmanları Komitesi (UNESC) - Tehlikeli Malların Taşınması

Erişilebilir Olması Gereken Referans Materyaller

- Mektup Postası El Kitabı
- Paket Postası El Kitabı
- S58 - Posta Güvenliği Genel Güvenlik Önlemleri
- S59- Değişim Ofisi ve Uluslararası Havayolu Güvenliği
- UPU Operasyonlar ve Teknoloji Müdürlüğü (DOT) Mektup Yönergeleri

Modül 2: S58-Posta Güvenliği Standartları- Genel Güvenlik Önlemleri

Modüle Giriş

Bu modülde şu hususlara değinilecektir.

- UPU güvenlik standartları nasıl ve neden geliştirildi?
- Kritik tesisin tanımı
- Minimum fiziksel güvenlik ve işlem güvenliği gereksinimleri
- Posta güvenlik birimi nasıl oluşturulur?
- Güvenlik bilinci programları nasıl geliştirilir ve uygulanır?
- Uygunluk denetiminin ne olduğu ve ne sıklıkta yapılması gerektiği
- Afet kurtarma, acil durum hazırlığı ve iş sürekliliği planlamasının temel kavramları

S58- Standarda Kısa Bir Giriş

- UPU anketi sonuçları, farklı bölgelerde uygulanan farklı yaklaşımların ve düzenleyici usullerin olduğunu ortaya koydu.
- Örneğin:
    - ✓ Dünya Gümrük Örgütü Güvenlik Standartları Çerçevesi
    - ✓ Uluslararası Sivil Havacılık Örgütü Standartları ve Önerilen Uygulamalar
- Farklı standartlarda ele alınan postalar için tek bir uluslararası standarda doğru evrilmek önemlidir.

S58 - Standarda Kısa Bir Giriş

- Posta işlemlerinin bir gümrük acentesi, havayolu şirketi veya havaalanı işlemi olmadığını akılda bulundurarak, hem posta işlemlerine duyarlı hem de diğer yönetimlerle uyumlu standartlara sahip olmak önemlidir.

- Posta menşeini kolayca belirleyen bir yaklaşımı benimseyen uluslararası bir standarda doğru evrilmek, transit posta konusunu daha az karmaşık hale gelmektedir.
- Belirlenmiş işletmecilerden, farklı ülkelerde hâlihazırda yürürlükte olan fiziki güvenlik ve tarama önlemleri hakkında temel bilgiler toplanmıştır.

Kilit Paydaşlar

- Uluslararası Sivil Havacılık Örgütü (ICAO)
- Uluslararası Hava Taşımacılığı Birliği (IATA)
- Dünya Gümrük Örgütü (WCO)
- Ulaştırma Güvenliği İdaresi (TSA)
- Avrupa Komisyonu
- Bazı Anahtar UPU üyeleri

Bu Paydaşlar Önemlidir, Çünkü;

- UPU'nin önemli tedarik zinciri ortaklarıdır
- Postaların taşınmasında kilit direktifler uygulamaktadırlar
- Tedarik zinciri ve taşıma esnasındaki tehditlere yönelik bilgi birikimini arttırırlar
- Posta hizmetlerinin güvenli ve verimli bir tedarik zinciri ile sağlamak için paydaşlar arasında uyum olmalı

Standartlar Neden Olmalı?

- UPU ve üyeleri, tek bir ses olarak hareket ederken çok daha güçlüdür.
- Posta iş modeli ile uyumlu standartlar oluşturmamız bizim için daha faydalıdır.
- Dışarıdaki kuruluşların standartlar empoze etmesi istenmiyor
- Uluslararası posta ağlarının güvenliğinin arttırılması iyi bir iş modelidir.

1 Ocak 2014 İtibariyle UPU Güvenlik Standartları Zorunludur (Madde 9 Posta Güvenliği)

Üye ülkeler ve belirlenmiş işletmeciler UPU güvenlik standartlarında tanımlanan güvenlik gerekliliklerini yerine getirecek ve vatandaşların posta hizmetlerine, olan güvenini korumak ve arttırmak için, tüm posta işlemlerinde ilgili tüm kurumlar yararına, proaktif bir güvenlik stratejisi benimseyip uygulayacaktır.

Genel Güvenlik Önlemleri

Terimler ve Tanımlar

- Erişim kontrolü - fiziksel güvenlik içerisinde, bir mülke, bir binaya veya bir odaya girişi yetkili kişilerin erişimine sınırlama uygulaması anlamına gelir.
    - ✓ Fiziksel erişim kontrolü, bir insan (bir güvenlik görevlisi veya resepsiyonist), kilitler ve anahtarlar gibi mekanik araçlar veya bir kartlı erişim sistemi gibi teknolojik araçlar aracılığıyla gerçekleştirilebilir.
- Belirlenmiş işletmeci - posta hizmetlerini yürütmek ve Birlik Yasaları topraklarında ortaya çıkan ilgili yükümlülükleri yerine getirmek için üye ülke tarafından resmen tayin edilen resmi ya da devlet dışı kuruluşlar.
- Kritik tesis – Değişim ofisi; havayolu birimi; havacılık güvenlik taramasının yapıldığı posta tesisleri; posta öğelerinin hava yoluyla gönderilmeden önce geçtiği son posta tesisi.
    - ✓ Not: Buradaki tanım, bu standartların uygulanması içindir, ancak gönderiler, diğer yerleri kendi iç risk değerlendirmesine dayalı olarak kritik tesisler olarak belirleyebilir (örnekler: işleme tesisleri veya finansal birimler).
- Minimum güvenlik gereksinimi - kritik öneme sahip tesis içinde yerel mevzuat, iç politika ve prosedürlerle ilgili güvenli operasyonlar sağlamak için uygulanacak asgari önlemlerden oluşan teknik, yöntem, süreç veya faaliyet.
- Tarama - postanın, patlayıcıları tanımlamak ve / veya tespit etmek için tasarlanan teknik veya diğer müdahaleci olmayan araçlarla incelenmesi.

Genel Güvenlik Önlemleri

Genel Bilgi

- Kritik tesis tanımı posta şubelerine bırakılmıştır.
- UPU, değişim ofisi veya havaalanı posta birimini kritik bir tesis olarak değerlendirmektedir
- Her bir tesis için bir güvenlik planı olmalıdır

Genel Güvenlik Önlemleri

Risk Değerlendirme İlkeleri

- Her tesiste yıllık risk değerlendirmesi yapılmalıdır.
- Her tesis için yazılı bir güvenlik planı hazırlanmalı ve devamlılığı sağlanmalıdır.
- Risk değerlendirmesi, biriminizde yaşanması muhtemel güvenlik riskini belirlemeye yardımcı olacaktır.

- Tüm birimler, geçmişlerine göre çevrelerine bağlı olarak farklı risklere sahip olacaktır.
- Risk ve tehditler sürekli değiştiği için riskin tamamen ortadan kaldırılması mümkün değildir
- Sürekli ihtiyatlı olmak ve stratejide değişiklik yapmak gereklidir.
- Zaten yürürlükte olan risk azaltma önlemlerinin ve bunların etkili olup olmadıklarının değerlendirilmesine yardımcı olacaktır.
    - ✓ Örneğin: CCTV sistemleri, alarmlar, acil durum planları, çalışanların eğitimi ve farkındalığı.
- Mevcut risk azaltma önlemlerinde var olan boşlukları belirleyecektir.
- Tehditlere risk seviyesi belirlenmesini sağlayacaktır
- Kaynakların mülk ve malvarlığı değerini ve yenileme veya yokluk maliyetlerini belirler.
- Mevcut binaları / tesisleri, personeli, ekipmanı, postayı, finansmanı ve envanteri kapsar.
- Neyin korunması gerektiğini ve koruma düzeyini belirler
- Yönetimden, çalışanlardan, kolluk kuvvetlerinden ve devlet kurumlarından malumat almaya ihtiyacı vardır.

Sorulacak Örnek Sorular

- Site içerisinde neler var?
- Bu bölgedeki suç faaliyeti nedir?
- Bu bölgede başka hangi tesisler var, ne gibi sorunlar yaşadılar ve güvenlik düzeyleri nedir?
- Tesis tasarımında ve yapımında ele alınması gereken güvenlik endişeleri nelerdir?

EKLER 2.1 Güvenlik Riski Değerlendirme Matriksi ↓

Genel Güvenlik Önlemleri

Tesis Güvenlik Planı

- Kritik tesis, tasarım standartları
- Çevre pencereleri kapıları veya diğer açıklıklar
- Kilitleme mekanizmaları ve anahtar kontrolleri
- Erişim kontrolü önlemleri
- Aydınlatma
- Çevre engelleri

EKLER 2.2 Tesis Güvenlik Planı

Genel Güvenlik Önlemleri

Kritik Çevre Tasarım Standartları

- Yıllık denetim ve risk değerlendirmesi
- Güvenlik ve emniyet için uluslararası standartlar oluşturulması

EKLER 2.3. Tesis Tasarım Standartları

Genel Güvenlik Önlemleri

Kritik Çevre Tasarım Standartları

Çevre bariyerleri, kapılar, pencereler ve aydınlatma

- Tesis bütünlüğünü sağlamak ve tamiratı yapmak için parmaklıklar, duvarlar ve araç kapıları kontrol edilmelidir.

- Çevre bariyerlerine bitişik alanlar enkaz, ağaç ve çalılıklardan uzak tutulmalıdır

- Çevre engelleri, yükseklik ve görünüm bakımından yerel kural ve düzenlemelerle sınırlandırılabilir.
- “Lütfen parmaklıklara tırmanmayın veya üstünden atlamayın” uyarısı asılmalıdır.

- Dış kapılar zorla girmeyi önlemek veya geciktirmek için yeterli dayanıklılığa sahip olmalıdır.

- Dış pencereler, kapılar ve diğer açıklıklar uygun kilitleme mekanizmaları ile güvence altına alınmalı ve bunların düzgün çalışıp çalışmadığı kontrol edilmelidir.

- Tüm yaya veya araç giriş / çıkış alanlarında, dış işletme alanlarında, park alanlarında ve çevre çitlerinde veya duvarlarda yeterli aydınlatma yapılmalıdır.

S58 Posta Güvenliği Standartları, Genel Güvenlik Önlemleri

Kilitler ve Anahtar Kontrolleri

- Kilitler, yetkili olmayan kişilerin erişimini engellemek için uygun malzemelerden yapılmalıdır.
- Yeterli derecede anahtar denetiminin sağlanmasını teminen sürekli bir anahtar kontrolü yapılmalıdır.

EKLER 2.4. Anahtar Logları ↓

S58 Posta Güvenlik Standartları, Genel Güvenlik Önlemleri

Personel İçin Erişim Kontrol Önlemleri

Genel

- Erişim kontrol önlemleri, kritik tesislerde posta ve posta araçlarına yetkisiz erişimi önleyecektir.
- Erişim kontrolü, güvenli alana giren bireyin veya aracın kimliğini doğrulamak için giriş ve çıkış noktalarında sabit güvenlik görevlileri kullanan manuel bir işlem olabilir.
- Erişim kontrol önlemleri, güvenli alanlara erişimi doğrulamak ve izin vermek için basit veya karmaşık elektronik sistemlerden de oluşabilir.
- Geçiş kontrol sistemi, çalışanlara, ziyaretçilere, servis sağlayıcılarına ve satıcılarına yalnızca iş işlevlerinin bulunduğu veya iş yaptığı alanlara erişim izni verir.
- Bir kayıt odası, herhangi biri girdiğinde harekete geçen bir ışık ve sesli uyarı veren çitle tamamen çevrili olmalıdır.

- Çalışan olmayan kişilerin güvenli alanlara girişlerini kaydetmek için bir ziyaretçi kayıt sistemi veya listesi tutulacaktır

- Kişisel eşyaların taşınması (cüzdanlar, sırt çantaları, vb.) ve bunların sınırlandırılmasının yanı sıra arama prosedürlerinin uygulanması da dikkate alınmalıdır.

- Güvenli alanlara kimlerin girdiğini görmek için kayıt günlüğüne sahip güvenli bir kayıtlı posta odası bulunmalıdır.

S58 Posta Güvenliği Standartları, Genel Güvenlik Önlemleri

Araçlar İçin Erişim Kontrol Sistemleri

- Bu alanlara giriş, tesisin sınırları konusunda karışıklığa neden olmayacak şekilde açıkça işaretlenmelidir.
- Manuel veya otomatik erişim kontrol sistemi kullanılmalıdır.

- Posta yüklemek / taşımak için kullanılan alanlarda veya diğer güvenli dış faaliyet alanlarında yalnızca resmi taşıtlara veya onaylanmış sözleşmesi olan araçlara izin verilmelidir

S58 Posta Güvenliği Standartları, Genel Güvenlik Önlemleri

Tanımlama Sistemleri

- Çalışanların ve ziyaretçilerin uygun bir şekilde tanımlanabilmesi için bir personel ve ziyaretçi tanımlama sistemi uygulanmalıdır.
- Posta personeline, insan kaynakları sisteminde belgelendirildiği şekilde yasal isimlerini, fotoğraflarını ve son kullanma tarihlerini içeren kolayca tanımlanabilen kimlik kartları verilemelidir.
- Erişim seviyesi, bölüm / birim gibi diğer bilgiler, yerel düzenlemeler ve mevzuatın gerektirdiği şekilde eklenebilir.
- Posta Güvenlik Birimi veya diğer posta yöneticileri, çalışan, ziyaretçi ve yüklenici kimlik kartlarının kontrolünden, çıkarılmasından ve kaldırılmasından sorumludur.
- Kimlik kartları iyi durumda olmalı ve görünebilecek şekilde takılmalıdır.

- Çalışanlara yönelik devam eden güvenlik eğitimi. Çalışanlara rozet takmalarını hatırlatan posterler asılmalıdır.

S58 Posta Güvenliği Standartları, Genel Güvenlik Önlemleri

Personel Güvenliği, Eğitimi ve İşe Alım Uygulamaları

Genel

- Çalışanlar bir güvenlik planındaki ana varlıktır.
- Çalışanlar ayrıca en büyük potansiyel güvenlik risklerini oluşturabilir.
- Personelin güvenliği ve eğitimi riski azaltmak için kritiktir.
- Bu sadece ilk istihdam aşamasında değil, çalışan ilerledikçe ve organizasyonda farklı roller üstlendikçe de önemlidir. Örneğin, insan kaynağına veya bilgi teknolojisi pozisyonlarına geçen çalışanlara ek eğitim ve sicil kontrolleri gerekebilir.
- İşe alım politikası, ana tesislerde çalışan veya harici yerlerde postaları işleyen tüm çalışanlar için belgelendirilmelidir.
- İstihdam politikası, posta görevlerini yerine getirmeye yetkili personelin uygun kişiler olmasını sağlamak için ulusal yasalarla tutarlı olmalıdır.
- Tüm kariyer çalışanlarına yönelik geçmiş kontrolleri (cezai tarihçesi veya polis kontrolleri), ulusal mevzuata uygun olarak yapılmalıdır.
- Çalışan performansını ve suistimalleri rapor etmek ve bildirmek için işlemler tesis edilmelidir.
- İşe alım süreci, görüşmeleri, iş öncesi veri doğrulamasını ve pozisyona veya görevlere bağlı olarak diğer önlemleri kapsamalıdır.
- Fesih süreci, çalışanlar ve yükleniciler için belgelendirilmelidir.
- Fesih süreci, kimlik belgelerinin, erişim kontrol cihazlarının, anahtarların, üniformaların ve diğer hassas bilgilerin iade edilmesini teminat altına almalıdır.
- Yanlış davranış nedeniyle işten çıkarılan çalışanların veya yüklenicilerin yeniden işe alınmasının önlenmesi için bir kayıt sistemi kullanılmalıdır.

S58 Posta Güvenliği Standartları, Genel Güvenlik Önlemleri

Yüklenici Güvenlik Gereksinimleri

- Posta elleçleme / taşıma işlemleri veya diğer hassas işlevleri yerine getirmek için kullanılan yükleniciler,posta işletmecilerine benzer personel güvenlik önlemleri uygulamalıdır.
- Yüklenici, operasyon için potansiyel güvenlik riskleri oluşturabilecek personel bulguları veya kararları hakkında işletmeciyi bilgilendirmelidir.

S58 Posta Güvenliği Standartları, Genel Güvenlik Önlemleri

Farkındalık ve Eğitim Önlemleri

- Güvenlik devam eden bir süreçtir.
- Çalışanların işe ilgilerinin devamı için hatırlatmalar ve eğitim önemlidir.
- Güvenlik kavramı organizasyon kültürünün bir parçası haline gelmelidir.
- Güvenlik herkesin sorumluluğundadır

- Çalışanlara güvenlik kaygıları ve mevcut güvenlik planları hakkında güncel bilgiler verilmeye devam edilmelidir.

- Çalışanlar için devam eden güvenlik eğitimi. Çalışanlara işyeri güvenliği hakkında hatırlatma posterleri

EKLER 2.5. Sürekli Güvenlik Önlemleri ↓

S58 Posta Güvenliği Standartları, Genel Güvenlik Önlemleri

Taşıma ve Sevk Güvenlik Gereksinimleri

- Belirlenmiş işletmeci ve yetkili yükleniciler, postanın güvenliği için tüm işlemleri ulaşımın her yolu (hava, kara, deniz ve demiryolu) için belgelendirmelidir.
- Belirlenmiş işletmeci emniyet ve güvenlikle ilgili ulaştırma standartlarına ilişkin geçerli tüm ulusal mevzuata uymalıdır.
- Postaya erişim posta çalışanlarına veya posta işlem sorumlulukları olan yüklenicilere uygun olarak sınırlandırılmalıdır.
- Posta taşıma araçları, dayanıklı malzemelerden tasarlanacak ve sağlam, sert üst veya sağlam yumuşak yanlar ve kilitli kargo kapıları gibi özelliklere sahip olmalıdır.
- Mümkün olduğunda, KCP97KM-7 Taşıtları veya nakil araçları, yetkili bir posta aracı veya yüklenici araç olarak açıkça işaretlenmeli veya tanımlanmalıdır.

- Araçlar yüklenmeden önce kontrol edilmeli ve herhangi bir kurcalama veya hasar belirtisi rapor edilmelidir
- Posta yüklü araçlar nakil halindeyken veya güvenli posta veya yüklenici tesislerinde gözetimsiz bırakıldığında, araç ve postaya tüm erişim noktaları güvence altına alınmalıdır (kilitlenmelidir)

- Mümkün olduğunda, nakliye operatörleri (posta veya yüklenici) belirlenmiş bir postacı üniforması giymeli ve / veya geçerli bir posta veya yüklenici tanımlaması biçimine sahip kimlik kartı taşımalı ve bunu açıkça göstermelidir.
- Taşıma araçlar yetkisiz kişilerin erişimine karşı korunmalıdır.
- Taşıtlar, nakliye araçları veya koliler uygun şekilde boşaltılmalıdır.
- Çantaların ve kolilerin uygun şekilde mühürlenmesi, etiketlenmesi ve sabitlenmesi nakliye sırasında posta güvenliği için kritik öneme sahiptir.

S58 Posta Güvenliği Standartları, Genel Güvenlik Önlemleri

Uygunluk Denetim Programı

Yıllık Uygunluk Denetimleri Yapılmalıdır.

- Denetim ekibine, ilgili bilgiyi elde etmek ve düzeltici önlemleri almak için gerekli yetki verilmelidir.

- Belirlenmiş işletmeci uygunluk denetim gözden geçirme programının yönetiminin, güvenlik gerekliliklerinin uygulanmasından sorumlu olan kişilerden bağımsız olmasını sağlamalıdır.
- Uygunluk denetim ve tavsiyelerinin kayıtları tutulmalıdır.
- Uygunluk denetimlerinin sonucu belirlenmiş işletmecinin yönetim kadrosuna bildirilmelidir. Takip işlemleri izlenmeli ve belgelendirilmelidir.

EKLER 2.6. Değerlendirme Gereci ↓

S58 Posta Güvenliği Standartları, Genel Güvenlik Önlemleri

Posta Güvenlik Birimi

- Belirlenmiş işletmeci postanın, çalışanların, ortakların, müşterilerin ve posta varlıklarının korunmasına yönelik önleme ve soruşturma alanlarını kapsayan belgelenmiş bir güvenlik programına sahip olmalıdır. Bu, tüm çalışanlara iletilmelidir.

  ✓ ÖRNEK: Ekipman, araçlar, üniformalar, bilgi teknolojisi vb.
- Belirlenmiş işletmeci güvenlik ve emniyet önlemlerini almak için özel bir Posta Güvenlik Birimi veya özel bir personele sahip olmalıdır. Bu fonksiyonlara tahsis edilen personel sayısı belirlenmiş işletmecinin büyüklüğü ve faaliyetleriyle orantılı olmalıdır.
- Posta Güvenlik Biriminin yapısı ve büyüklüğü görev yerinin ihtiyacına bağlı olacaktır.
- Birim, güvenlik programlarını incelemek ve uygulamak için atanmış bir güvenlik grubu veya bir komite olabilir
- Güvenlik, tüm çalışanların sorumluluğunda olmalıdır.

Posta güvenlik birimi / komitesi örneği, farklı bölümdeki üyeleri içerebilir.

S58 Posta Güvenliği Standartları, Genel Güvenlik Önlemleri

Afet Kurtarma, Acil Durum Hazırlığı ve İş Sürekliliği Planlaması

- Belirlenmiş işletmeci uygun çalışanları belgelendirmeli ve onlarla iletişime geçmelidir:
- Posta veya posta işlemlerinin akışını etkileyecek insan kaynaklı veya doğal bir felaket durumunda posta, çalışanlar, müşteriler ve posta varlıklarının güvenliğini sağlamak için bir kriz planı;
- Yerel veya uluslararası posta operasyonlarını etkileyebilecek önemli bir olay durumunda posta kesintisini en aza indirecek bir iş sürekliliği planı hazırlanmalıdır.

- İş sürekliliği planlaması, krizin yönetilebilmesi ve kurumun bekasının sağlanması amacıyla, birimlerin krize hazırlanmak için gerekli önlemleri ve faktörleri göz önüne almasını sağlar.
- Afet veya acil durum örnekleri:
  - ✓ Grevler/darbeler
  - ✓ Doğal Afetler (Kasırgalar, Tayfunlar, Depremler)
  - ✓ Elektrik Kesintileri
  - ✓ Bombalama
  - ✓ Siber saldırı
- Acil durum müdahale planı, iş sürekliliği planının bir parçasıdır ve acil durumlara ilk müdahale için gerekli süreci sağlar.

• Bu planlar tipik olarak aşağıdakilerle ilgili bilgileri içerecektir:

Tahliye; Bir yerin ne zaman ve nasıl güvenli bir şekilde tahliye edileceği

Barınma; Şiddetli hava koşulları veya diğer güvenlik tehditleri durumunda korunacak yerler

Yerinde Barınma; Belirli bir yere nasıl sığınılacağı

Kilitleme; İşyerinde şiddet varsa, çalışanlar tarafından ne yapılması gerektiği

Şüpheli Maddeler; Şüpheli posta eşyalarının bulunması durumunda ne yapılması gerektiği

- Afet kurtarma aynı zamanda iş sürekliliği planının bir parçasıdır ve büyük kesintilerden kurtulmak için süreç sağlar
- Plan, bir felaketin yol açtığı zararları en aza indirmek ve toparlanma sürecine başlamak için işletme tarafından atılacak adımları içermelidir.
- Kritik iş işlevlerini çalışabilir hale getirmek ve organizasyonu kabul edilebilir bir duruma getirmek için tasarlanmış etkinlikleri ve programları içerir.

EKLER 2.7. UPU Kriz Planlaması ↓
EKLER 2.8. Acil Durum Hazırlık ↓
EKLER 2.9 Tehlikeli Madde Eylem Planı ↓

Modül 3: S59- Posta Güvenlik Standartları- Borsa ve Uluslararası Havayolu Ofisi

Terimler ve Tanımlar

Bu modülde aşağıdaki hususlar açıklanacaktır.

- Minimum posta tarama standartları gereksinimleri
- Güvenli tedarik zincirinin tanımı
- Yüksek riskli maddelerin kriterleri
- Şüpheli postalar için alarm ve çözme işlemi

TERİMLER VE TANIMLAR

BÖLÜM 5: TARAMA STANDARTLARI

BÖLÜM 6: TİCARİ HAVAYOLU TAŞIMACILIĞI İÇİN ALINAN/KABUL EDİLEN POSTALAR İÇİN ÖNLEMLER

Terimler ve Tanımlar

- Sevkiyat – belirli bir posta kategorisine ait bir veya daha fazla paket/zarfın belirli bir durumda, belirli bir yükleme noktasından belirli bir son varış yerine kadar toplu nakil yoluyla taşınması.
- Patlayıcı tespit sistemi (PTS) - bagajda veya diğer eşyalarda bulunan patlayıcı malzemeleri tespit etme kabiliyetine sahip teknoloji sistemi veya farklı teknolojilerin kombinasyonu.
- Patlayıcı tespit köpeği (PTK) - patlayıcıları tespit etmek için eğitilmiş köpek
- Patlayıcı iz tespiti (PİT) - patlayıcı izlerini tespit etmek amacıyla, ayrı ayrı postalardan parçacık numunelerinin toplandığı ve patlayıcı kalıntı izlerini tespit etmek için bir PİT makinesi aracılığıyla postaların içeriklerini taramak için kullanılan teknoloji
- Yasaklanmış madde - yasadışı eylemlerde kullanılabilecek patlayıcı veya yanıcı maddelerin bütünü ve parçaları.

Not: Bu tanım, bu standartları uygulamak amacıyla kullanılabilir.

- Tarama - postaların, patlayıcıları tanımlamak ve/veya tespit etmek için tasarlanan teknik veya diğer zorlayıcı olmayan araçlarla incelenmesi.
- Güvenli tedarik zinciri – postaların, tedarik zincirinde emniyete alınmasını, güvenli bir ortamda taşınmasını ve hava taşıyıcısına güvenli olarak teslim edilmesini sağlayan model.
- Ulusal Sivil Havacılık Güvenliği Programı (NCASP) - tipik olarak her ülke, havacılık güvenliğinin bir parçası olarak yasaları, politikaları, programları ve düzenlemeleri belirleyen bir Ulusal Sivil Havacılık Güvenliği Programı kurmuş olacaktır. Havacılık sisteminin güvenliğinin yasadışı müdahalelerden korunması, böylece hava taşımacılığı ve ticaretin güvenliği sağlanmış olacaktır.

5- Tarama Standartları

ULUSLARARASI POSTALARIN MUHAFAZASI

TARAMADAN MUAF OLAN MADDELER

TARANMASI GEREKEN MADDELER

YÜKSEK RİSK TAŞIYAN MADDELER

POSTA ZARFLARINI VE PAKETLERİNİ TARAMA PROSEDÜRLERİ

ŞÜPHELİ MADDELERİN ALARM ÇÖZÜMLEMESİ

İHBAR PROSEDÜRLERİ

5.1- Uluslararası Postaların Muhafazası

- Belirlenmiş işletmeci postaların kabul zamanından taşıyıcıya/acenteye/görevli birime gönderimine kadar kontrolü elinde tutar.
- Bir belirlenmiş işletmeci kendi adına posta kabul etmek için bir yüklenici veya başka bir yetkili kullanıyorsa, belirlenmiş işletmeci hala postadan sorumludur.
- Belirlenmiş işletmeci yüklenicinin veya görevli firmanın da bu standartlara uymasını sağlamalıdır.

5.2 - Taramadan Muaf Olan Maddeler

- Bazı durumlarda, yerel Ulusal Sivil Havacılık Güvenliği Programı'ları, ek tarama yapılmadan 500 grama kadar uluslararası postaların gönderilmesinde serbestlik tanıyabilmektedir.
- UPU üyesi ülkeler, bazı posta türlerinin doğası gereği özel olması nedeniyle, bunların taramadan veya alternatif güvenlik önlemlerinin kullanılmasından muaf tutulmasına izin vermeyi kabul edebilir.
- Bu istisnalar, UPU üyesi ülkelerin Ulusal Sivil Havacılık Güvenliği Programı'larında açıkça tanımlanmalıdır.
- Ulusal Sivil Havacılık Güvenliği Programı tarafından muaf tutulabilecek öğelere örnekler:
  - ✓ Yüksek değerli ürünler
  - ✓ Viyana Sözleşmesi hükümlerine uygun olan diplomatik posta
  - ✓ Besi hayvanı veya evcil hayvan gibi canlı hayvanlar

- Aşılar ve diğer bozulabilir tıbbi ürünler
- Kan, kan ürünleri, kemik iliği ve yetkili kuruluşlardan gelen nakil amaçlı insan organları gibi hayati ürünler
- İnsan kalıntıları
- Özel nükleer maddeler

5.3 - Taranması Gereken Maddeler

- Posta taraması, Sivil Havacılık Güvenliği Programı göz önünde bulundurularak yapılmalıdır
- Yasaklanmış ürünleri tespit etmesi en muhtemel araçlar veya yöntem (UPU posta güvenlik standartlarında tanımlandığı şekilde), paketin veya maddenin niteliği göz önüne alınarak uygulanmalıdır.
- Kullanılan araçlar veya yöntem, pakette veya gönderide yasaklanmış maddelerin gizlenmemesini sağlamak için geçerli bir standartta olmalıdır.
- Paketlerde veya gönderilerde yasaklanmış madde bulunmadığı makul bir şekilde tespit edilemezse, bu gönderiler reddedilmeli veya yeniden taranmalıdır.
- Tarama işini yürüten tüm personelin eğitimli olması ve denetlenmesi gerekmektedir.
- Tarama ekipmanlarının korunması, denetlenmesi ve üreticinin yönergeleri doğrultusunda kullanılması gereklidir
- Belirlenmiş işletmeci veya görevli firma, gönderileri Sivil Havacılık Güvenliği Programı'larında ve bu standartta belirtilen yöntemlerden en az birini kullanarak taramalıdır.
- Birden fazla tarama yönteminin bulunması faydalı olacaktır.

5.3 Tarama Yöntemleri

- PTK ve Tespit Köpekleri
- PİBT Patlayıcı İz ve Buhar Tespiti Metal Tespiti
- PTS - Patlayıcı Tespit Sistemi
- Elle İnceleme / Gözle inceleme
- X-Ray cihazı veya diğer dalga tabanlı sistemler

X-Ray ve Gözle İnceleme

Patlayıcı ve Buhar İzi İnceleme

5.4 - Yüksek Risk Taşıyan Maddeler

- Temel prosedürlerin ötesinde ek güvenlik önlemleri gerektiren postalar yüksek riskli maddeler olarak değerlendirilir
- Belirli kriterleri karşılayan posta veya posta maddeleri yüksek riskli olarak kabul edilir

Kriterler

- Kurcalama veya hasar gibi delillerle şüpheye yol açan uygunsuzluklar
- Tek başına temel güvenlik önlemlerinin, UPU posta güvenlik standartlarında tanımlandığı şekilde yasaklanmış maddeleri saptamasının mümkün olmadığı durumlar.

- Bir madde hakkında özel istihbarat veya tehdit bilgisi
- Havacılık güvenliği, uçak işletmecileri, kolluk kuvvetleri makamları veya tedarik zincirindeki diğer aktörlerden alınan istihbarat veya bilgiye dayalı bir tehdit olduğuna dair şüpheye sebep olan durumlar

- Belirlenmiş işletmeci veya görevli firma, yüksek riskli maddeleri aşağıdakilere göre tarar:
  - ✓ Maddeyi iki farklı açıdan görme ve ulusal mevzuata uyma, veya;
  - ✓ Aşağıdaki tarama yöntemlerinden iki veya daha fazlasının bir kombinasyonunu kullanma:

ELLE TARAMA	X-RAY EKİPMANLARI	PATLAYICI TESPİT KÖPEKLERİ	PATLAYICI İZ TESPİTİ

5.5 Posta Paketleri/Torbalar İçin Tarama Prosedürleri

- Kendi ulusal kurumları tarafından yetkilendirildiğinde belirlenmiş işletmeci veya görevli firma, paketlerde/torbalarda bulunan maddeleri taramak için geçerli teknolojileri kullanmalıdır
- Birçok ülkede posta taraması izni, genellikle ulusal sivil havacılık otoritesi tarafından idare edilen düzenlenmiş bir acente programından veya eşdeğer başka bir programdan gelir.

Mevcut Teknoloji

- Belirli bir ürün veya paket için en uygun x-Ray tarama teknolojisi
  - ✓ Belirlenmiş işletmeci yasaklı malların taramak için bir seferde bir paketin x-ray görüntünü almalıdır.
  - ✓ Doğru bir x-ray görüntüsü oluşturmak için fazla yoğun olan maddeleri içeren postalar, üreticinin önerisine göre iki kez taranmalıdır
  - ✓ X-ray görüntüsü net değilse, belirlenmiş işletmeci her bir posta parçasını paketten çıkararak temiz bir x-ray görüntüsü elde etmeye çalışmalı ve parçaları tek tek taramalıdır.
- Patlayıcı Tespit Köpekleri
- Patlayıcı Tespit Sitemleri

5.6 Şüpheli Maddelerin Alarm Çözümü

- Belirlenmiş işletmeci veya tarama görevlisi, ilk tarama sırasında güvenli olduğu tespit edilemeyen (alarm) bir madde tanımlarsa, paket "Uçmak İçin Güvenli" olduğu tespit edilene kadar bir taşıyıcıya teslim edilmemelidir.
- Madde, bu standardın 5.4 maddesine göre yüksek riskli bir madde olarak ele alınmalıdır.

5.6 Şüpheli Maddelerin Alarm Çözümü "Risk Değerlendirmesi Uygulaması"

Aşağıdakileri kullanarak her bir parça yeniden taranmalıdır.

X-ray ekipmanları	PTK	Posta içeriğini PİT kullanarak tara	PTS

Dikkate Alınması Gereken Seçenekler

- Güvenilir olduğu tespit edilemeyen maddeleri işlemek için yazılı prosedürler veya protokoller bulunmalıdır.
- Hayati anlamda ve sağlık için önemli bir tehlike olmadığı belirlenmeli
- Eğer güvenliyse, içeriği doğrulamak için gönderen ve/veya alıcı ile sözleşme yapılmalı
- Sivil Havacılık Güvenliği Programı'nın veya yerel kanun ve yönetmeliklerin yönlendirdiği şekilde yerel yetkililere başvurulmalıdır.

5.7 Bildirim Prosedürleri

- Sivil Havacılık Güvenliği Programı'nın gereklilikleri konusunda, belirlenmiş işletmeci veya tarama sorumlusu bir ürünün güvenli olduğunu tespit edemezse posta, herhangi bir taşıyıcıya / uçağa teslim edilmemeli, yüklenmemeli veya taşınmamalıdır.
- İzinsiz girişleri önlemek için ürün güvenli bir yerde izole edilmeli, kontrol edilmeli ve fiziksel olarak korunmalıdır.
- Belirlenmiş işletmeci veya tarama görevlisi:
    - ✓ Yerel gerekliliklere uygun olarak hemen Yer Güvenlik Koordinatörü (YGK), ev sahibi hükümet yetkilileri, polis, itfaiye ve / veya bomba imha ekibi ile irtibata geçilmelidir.
    - ✓ Şüpheli postayla birlikte getirilmiş veya nakledilmiş olan ek bir uluslararası posta tespit edilmesi durumunda ilgili kurumlar bilgilendirilmelidir

Değişim Ofisi ve Uluslararası Havayolu

6- Ticari uçak nakli için kabul edilmiş/alınmış postalar için önlemler

- Belirlenmiş işletmeci postaları taşıyıcılara, yer taşıma görevlisine ve yükümlü firmaya tanınabilir çantalar (torbalar) veya uygun UPU formları ve/veya paket etiketleri yapıştırılmış torbalarda dikkatli şekilde ulaştırmalıdır.
- Tüm paketlere/gönderilere, uygun UPU dokümantasyonu veya bunun eşdeğeri olan elektronik belge eklenmelidir.

UPU Belgelendirmesi

- Havaalanında teslim edilen postalara, kara veya denizden giden/adi (S.A.L.) postalarda, CN 38 teslimat faturası veya CN 41 kopyaları eklenmelidir.
- Havayolu taşıma torbalarında CN 35 etiketi
- Hava ile yüzeye çıkan torbalar (S.A.L) CN 36 etiketi.
- Hava koli postası CP 84 etiketi.
- Hava ile yüzeye çıkan torbalar CP 85 etiketi (S.A.L.) koli postası

Havaalanında teslim edilen postalara, kara veya denizden giden/adi (S.A.L.) postalarda, CN 38 teslimat faturası veya CN 41 kopyaları eklenmelidir.

- Havayolu taşıma torbalarında CN 35 etiketi
- Hava ile yüzeye çıkan torbalar (S.A.L) CN 36 etiketi.

- Hava koli postası CP 84 etiketi.
- Hava ile yüzeye çıkan torbalar CP 85 etiketi (S.A.L.) koli postası

Döviz Bürosu ve Uluslararası Havayolu

6-Ticari Uçak Nakliyesi İçin Kabul Edilen/Tayin Edilen Posta Önlemleri

- Tarama veya diğer güvenlik kontrollerinin uygulanmasından sonra, posta işletmesi sorumlu olmalı ve yer taşıma acentesi veya diğer yüklenicilerden uçağa yüklemeden veya taşıyıcı ile güvenli değişimden önce yetkisiz girişime karşı korumalıdır.
- NCASP uyarınca, uçak operatörüne bir sevkiyat güvenlik bildirimi sağlamak için tarama ve güvenlik kontrolleri uygulayan bir belirlenmiş işletmeci gerekebilir.

Uluslararası Giden Posta Tarama Akış Şeması

Posta Güvenliği

Modül 4: Postadaki Tehlikeli Mallar

Modülün Amacı

Bu kurs tamamlandığında aşağıdaki hususlar açıklanıyor olacak

- Tehlikeli maddeleri tanımlama
- Tehlikeli maddeleri dokuz kategorisini tanımlama
- Postada hangi tehlikeli maddelere izin verildiğini belirleme

- Tehlikeli maddeler içerebilecek ortak öğeleri tanımlama
- Postada tespit edilen tehlikeli maddelerin taşınması için uygun prosedürleri tanımlama
- Çalışan eğitimi veya farkındalık programının gerekli unsurlarını tanımlama
- Müşteri farkındalık stratejileri oluşturma ve uygulama

Tehlikeli Maddeler Nedir?

- Tehlikeli maddeler taşınırken sağlık, güvenlik, mal veya çevre için risk teşkil eden eşya veya maddelerdir.
- Tehlikeli maddelerin kara, demiryolu, deniz ve hava yoluyla taşınmasına ilişkin uluslararası düzenlemeler vardır.
- Bu düzenlemeler, tehlikeli maddelerin güvenli bir şekilde taşınabileceği prosedürleri ve gereksinimleri içerir.
- Nakliye şekline bağlı olarak taşınabilecek tehlikeli maddeler için özel ambalajlama gereklilikleri ve hacim / kitle kriterleri vardır.
- Dokuz tehlikeli madde sınıfı vardır. Neredeyse tüm tehlikeli maddelerin uluslararası posta ile taşınması yasaktır.
- Tehlikeli maddelerin gönderilmesinin engellenmemesi nakliye sırasında ciddi kazalara neden olabilir.
- Tehlikeli maddeler ayrıca belirlenmiş işletmeciler tarafından ele geçirilebilir ve bertaraf edilebilir, müşteriye rahatsızlık verebilir ve gelecekte iş kaybına neden olabilir.
- Düzenleyiciler, doğru prosedürlere uyulduğundan emin oluncaya kadar bir belirlenmiş işletmeciyi cezalandırma ve yetkisini askıya alma gücüne sahiptir.

Tehlikeli Maddeler Bulunduğunda

- Hızlı posta kargosu
- Tehlike etiketi ile açıkça işaretlenmiş
- Bir belirlenmiş işletmeci tarafından kabul edilen

Tehlikeli Maddelerin Dokuz Sınıfı

1. Patlayıcılar

- • Havai fişekler, maytaplar, fişekler, mühimmat, parti patlayıcıları, otomobil hava yastıkları

2. Gazlar

- Aerosoller (örneğin oda spreyleri), kamp gaz tüpleri, sigara çakmakları, saç düzleştiricilerindeki bütan dolgusu

3. Yanıcı Sıvılar

- Benzin / petrol, benzinli çakmak, parfüm, yüksek alkol içerikli alkollü içecekler (>% 24 ABV), tırnak cilası sökücü

4. Yanıcı Katı Maddeler, Kendiliğinden Yanmaya Neden Olabilecek Maddeler; Su ile Temas Halinde Yanıcı Gazlar İçeren Maddeler

- Kibritler, ateşleme çakmakları, işaret fişekleri, yağlı gaz

5. Oksitleyici Maddeler; Organik Peroksitler (Oksijenli Su)

- Çamaşır suyu, araç tamir takımları, amonyum nitratlı gübre

6. Zehirli ve Bulaşıcı Maddeler

- Böcek ilacı, yabancı ot öldürücüler, zehirler, bulaşıcı kan

7. Radyoaktif Madde

- Hava aracı gibi ışıklı kadranlar

8. Aşındırıcı Maddeler

- Akü asidi, lavabo açıcı, cıva (örneğin bir barometrede bulunan)

9. Çevresel Olarak Tehlikeli Maddeler Dahil Olmak Üzere Tehlikeli Maddeler ve Nesneler

- Lityum piller, kuru buz, kendiliğinden şişen can kurtarma cihazları, güçlü mıknatıslar, jel piller (örnekler: golf arabaları, motorlu tekerlekli sandalyeler, engelli motosikletleri için)

EKLER 4.2. Avustralya Tehlikeli Posta Dokümanı ↓

EKLER 4.3. USPS Uluslararası Tehlikeli Posta Dokümanı ↓

Tehlikeli Madde Düzenlemeleri

- Birleşmiş Milletler ekonomik ve sosyal konsey uzmanlar komitesi (UNESC)
  - ✓ Tehlikeli malların nakliyesi için önerilerde bulunur, modeller hazırlar.
- Hava taşımacılığı ve nakliyesinde tehlikeli mallar
  - ✓ Uluslararası sivil havacılık örgütü (ICAO)
  - ✓ Evrensel Posta Birliği (UPU)

UNESCO Uzmanlar Komitesi

- "Tehlikeli mal düzenleme modelinin nakliyesine ilişkin tavsiyeler"
- Genel olarak "Turuncu Kitap" olarak anılır
- Tehlikeli malların taşınması için etiketleme ve ambalajlama usulleri vb. yönelik tavsiyeler yapar.

ICAO Teknik Talimatları

- ICAO teknik Talimatları tehlikeli maddelerin hava yoluyla güvenli şekilde uluslararası nakliyesi için gerekli detaylı talimatları içermektedir.

ICAO Tehlikeli Malların Hava Yoluyla Güvenli Taşınması için Teknik Talimatlar

- Tehlikeli malların uçak veya yolcuları tehlikeye sokmadan taşınabilecekleri güvenlik seviyesi sağlarken bu maddelerin kolayca taşınabilmesini amaçlamaktadır.
- Genellikle sivil havacılık otoritesi olan ulusal yetkili makamlar tarafından uygulanır. Bunlar her ülkede yönetmelik haline gelir
- DGR (Tehlikeli Madde Düzenlemeleri) ICAO'nun "montaj kılavuzu" sürümüdür.

IATA Tehlikeli Maddeler Düzenlemeleri (DGR)

- DGR, ICAO teknik Talimatlarının " montaj kılavuzu" sürümüdür
- Tehlikeli maddelerin hava yoluyla nakliyesi için gerekenler kullanıcı dostu ve yorumlaması kolay bir formatta sunulmuştur
- DGR ayrıca göndericilerin sevkiyatlarının uygun olduğundan emin olmalarına yardımcı olacak ve havayolları tarafından hızlı ve kolay bir şekilde kabul edilmesini sağlayan ek bilgiler içerir.
- DGR, bir gönderinin nasıl hazırlanacağını daha kesin olarak belirler.

Evrensel Posta Birliği Düzenlemeleri

- Uluslararası postalarla sınırlandırılmış tehlikeli maddelerle ilgili düzenlemeler posta mektubu ve kargo posta kılavuzlarında bulunmaktadır
- Özellikle RC 119 ve RL 131 istisnai olarak kabul edilen tehlikeli malları listeler.
  - ✓ Sınıf 7 - radyoaktif malzemeler
  - ✓ Sınıf 6.2-bulaşıcı Maddeler
  - ✓ Sınıf 9-ekipmanda bulunan lityum metal piller ve lityum iyon bateriler
- Üçü de, Teknik Talimatlar ve UPU kılavuzlarında yer alan özel limitler ve paketleme talimatlarıyla kabul edilir.

Uluslararası Postalarda Tehlikeli Maddeler

- Postalar, onlarca yıldır kabul edilebilir tehlikeli maddeleri taşıyorlardı ve zaten tehlikeli maddelere yönelik eğitimi ve kontrol süreçleri mevcuttur.
- Uluslararası Sivil Havacılık Teşkilatı (ICAO) Tehlikeli Maddelerin Hava Yoluyla Güvenli Taşınması için Teknik Talimatlar, postadaki tehlikeli malların hava taşımacılığına girişinin kontrol edilmesi için belirlenmiş posta işletmecileri prosedürlerinin postanın kabul edildiği devletin sivil havacılık otoritesinin incelemesine ve onayına tabi olmasını gerektirir.
- ICAO, 1 Ocak 2013 tarihinde yürürlüğe giren Teknik Talimatlarını değiştirmiştir.
- Özel Operatörler Gereksinimi belirlenmiş işletmeci
  - ✓ Postaların, Sivil Havacılık Kurumundan (CAA) özel onay almaları şartıyla, kabul edilebilir lityum pil içeren cihazları taşımasına izin verilir.
  - ✓ CAA'nın tehlikeli mal kontrollerini, kabul prosedürlerini ve eğitim programlarını incelemesi ve onaylaması gerekir.

Postadaki Tehlikeli Maddeler Nasıl Belirlenir?

- Çoğu durumda, çalışanınız bir müşterinin postalama için sunduğu bir paketin içini göremez
- Çalışanlar diğer tehlikeli maddelerin işaretlerini tanıyacak şekilde eğitilmelidir.
- Dokuz sınıfın etiketlerine ek olarak, bazı tehlikeli madde paketlerinde içeriklerin neden olduğu riski tanımlamak ve taşıyıcıların bunlarla nasıl başa çıkacaklarını bilmelerine yardımcı olmak için ek etiketler gerekir.
- Tehlikeli maddeleri içeren dış ambalajlar da, içindekiler UN harfleri ile yazılan dört basamaklı UN numarasından taşınmalıdır. Örneğin; UN1950
- Koargo aynı zamanda tehlikeli maddeleri tanımlayan elmas şeklinde bir tehlike etiketi taşıyabilir.

BM Tehlike Etiketleri

Ek Etiketler

Bu etiketler kargo olarak sunulan mallarda kullanılır, ancak bunlara uluslararası postalarda izin verilmez.

Nakliyatçı Beyanı

- Postayla taşınamayan çoğu tehlikeli mal, kargo olarak taşınırken "Gönderici Beyanı" olarak bilinen tehlikeli mal taşıma belgesini gerektirir.
- Bir müşterinin "Göndericinin Beyanı" ile birlikte bir eşya sunması, içeriğin tehlikeli mal olduğu anlamına gelir ve bu nedenle postada izin verilmemelidir.

Yeniden Ambalaj

- Bazen müşteriler tehlikeli madde etiketi taşıyan ambalajları yeniden kullanırlar
- Kolinin, tehlikeli ürünler içermediğini doğrulamak için müşterinin etiketleri veya işaretleri çıkarması, örtmesi veya ortadan kaldırması gerekir
- Bu, tedarik zincirinde hareket ederken paketin gereksiz alarmları tetiklemesini önleyecektir.

Formlardaki Açık Tanımları Arayın

A postal item can be accepted only if the description of the contents makes it clear that the item does not contain dangerous goods		
Examples of descriptions with which postal items cannot be accepted	Reason why unacceptable	Examples of descriptions with which postal items can be accepted
No description or vague description such as "miscellaneous goods", "daily commodity", or "precision instruments" Product serial numbers instead of descriptions	Contents are unknown	Wallets, compact discs
Household goods	May contain spray can or compressed gas cylinder	Food, clothing
Sporting goods	May contain aerosol	Racket, ball, shoes
Camping goods	May contain gas cylinder	Tent, sleeping bag
Diving goods	May contain a tank	Wet suit, hydroscope, snorkel
Medical drugs	May contain medical alcohol	Cold medicine, digestive medicine
Cosmetics	May contain flammable perfume, manicure goods, nail-polish remover	Soap, lipstick
Automobile components	May contain flammable fuel additives, aerosols, compressed gas	Mirror, seat cover
Toys	May contain batteries	Toy building blocks

Posta Ağına Tehlikeli Maddelerin Girişinin Kontrol Edilmesi İçin Prosedürler

- Tüm posta işletmecileri tehlikeli maddelerin posta ağlarına sızmasını kontrol etmek için prosedürlere sahip olmalıdır.
- CAA (Civil Aviation Authority, Sivil Havacılık Kurumu) bu prosedürleri hava taşımacılığının güvenlik ve emniyetinin bir parçası olarak inceleme yetkisine sahiptir.
- UPU, tehlikeli malların posta ağlarına sızmasını kontrol etmek için kılavuz materyal geliştirmiştir. Tüm posta kalemleri teknik talimatların gereklerine uygun durumdadır.

Rehberlik İşlevi İçeren Unsurlar

- Personel için tehlikeli mal eğitimi
- Sivil havacılık makamlarına ve / veya diğer ulusal makamlara tehlikeli mal kazalarını ve olaylarını rapor etmek ve takip etmek
- Gizli ve bildirilmemiş tehlikeli maddelerin sivil havacılık yetkililerine bildirilmesi
- Posta müşterilerini postayla kabul edilebilir olanlar hakkında bilgilendirmek için yöntemler
- Müşterileri tehlikeli mallarla ilgili kısıtlamalar ve yönetmelikler hakkında bilgilendirmek için yöntemler
- Acil durum prosedürleri
- Belgelerin saklanması
- Belgeli kabul prosedürleri
- Gönderen bilgisini gerektiren prosedürleri
- Reddedilen paketlerin yönetimi prosedürleri

EKLER 4.1.1'den 4.1.7'ye kadar USPS Güvenlik Afişleri ↓

EKLER 4.1.10. ve 4.1.11 Japonya Posta İdaresi Güvenlik Afişleri ↓

EKLER 4.1.12 ve 4.1.13 Danimarka Posta İdaresi Güvenlik Afişleri ↓

EKLER 4.1.14 ve 4.1.15 Kanada Posta İdaresi Güvenlik Afişleri ↓

EKLER 4.1. UPU Güvenlik Dokümanı ↓

Personel İçin Tehlikeli Madde Eğitimi

- Tehlikeli mal taşımayı tercih etmeleri gerekip gerekmediğine bakılmaksızın, belirlenmiş tüm işletmeciler tehlikeli maddelerin posta ağlarına girmesini ve muhtemelen hava taşımacılığı için teklif edilmesini önlemek için prosedürler uygulamaktadır.
- Bu prosedürlerin bir kısmı personel için tehlikeli mal eğitimini kapsamaktadır.
- Tehlikeli madde eğitim programları CAA tarafından gözden geçirilmeye ve onaylanmaya tabi tutulur.

- Eğitim programları, çalışanın görevleri ile ilgili olmalıdır (örneğin, gişe memuru ile posta işleyicisinin)
- Tekrarlayan eğitim kurulmalı ve CAA'nıza karar verilmelidir.
- Teknik talimatlardaki Tablo 1-6, belirlenen posta işletmeci personeli için önerilen kurs içeriğini sağlar;
- Çalışanlar üç kategoriye ayrılır:

  A posta kabul etmekte görevli personel

  B posta işleminde görevli personel

  C Postaların taşınması, depolanması ve yüklenmesinde görev alan personel

EKLER 4.4. ICAO teknik Enstitüsü Personel Eğitim Programı ↓

Müşteri Farkındalığı Yöntemleri

- Posta tesislerinde postayla izin verilen tehlikeli maddeler hakkında uyarı posterleri (resmi ve anlaşmalı ofisler)
- Posta temsilcileri tarafından müşteri için kısa bilgilendirme toplantıları
- İşletmeci web sitelerinde müşterilere uyarı bilgisi
- Müşterilere gönderilmiş uyarılar, reklamlar gibi diğer bildirimler

Zarar Görmüş veya Sızdıran Koli

- Şüpheli kolilere karşılık vermek için işletmeci prosedürleri olmalıdır
- Bu prosedürler organizasyonun tüm çalışanlarına iletilmelidir.
- Tehlikeli madde içeren bir koli zarar görürse, şüpheli koli prosedürlerine veya diğer uygun yerel prosedürlere uygun olarak işlemler yürütülmelidir.

◆ These plans will typically include information on the following:

Modül 5: Yasaklı Malların Postalanmasının Kötüye Kullanımı - Uyuşturucu Trafiği Hedefleri

Bu mödül sanunda aşağıdaki hususlar açıklanıyor olacaktır:

- UPU düzenlemelerini ve yasadışı uyuşturucu kaçakçılığını düzenleyen uluslararası yasalar
- Postaların yasadışı uyuşturucu trafiği için neden kullanıldığı
- Postadaki yasadışı uyuşturucuların ve gizlenme yöntemleri
- Postada yasadışı uyuşturucuları gönderme yöntemleri
- UPU Sözleşmesi Madde 18, kabul edilmeyen maddeler
    - ✓ 2.1.1 Uluslararası Narkotik Kontrol Kurulu tarafından tanımlandığı şekilde narkotikler ve psikoterapik maddeler veya varış ülkesinde yasaklanan diğer ilaçlar;
    - ✓ 2.1.5 Ambalajları gereği, çalışanları veya insanları tehlikeye maruz bırakabilecek, diğer eşyalara, posta ekipmanlarına veya üçüncü şahıslara ait mülklere zarar verecek veya kirletebilecek maddeler

Postada Neden Yasadışı Uyuşturucu Var?

- Güvenilirlik
- Kullanım kolaylığı ve nispeten düşük maliyetli
- Görünürlük (izleme)
- Ulusal yasalarla korunan postalar
- Özel kuryelerin daha katı posta gerekliliklerinin olması
- Evrensel hizmet yükümlülükleri
- Anonimliği
- Uyuşturucuların fiziksel olarak uluslararası bir sınırdan geçen bir insan kurye ile taşınmasından kaçınma

Küresel E-ticaret, Gizli Uyuşturucu Kaçakçılığı İçin Örtü Görevi Görüyor

- Posta mektubu hacmi birçok alanda düşerken, kargo hacmi çok hızlı bir şekilde artmaktadır.
    - ✓ Üreticiden kullanıcıya doğrudan teslimatı sağlar (küçük miktarlar)
    - ✓ Kaçakçılığın tespiti her zamankinden daha zor

title	price	seller	ship from	
NEW .1 Bag Of Heroin	฿5.87	dolfan2500(100)	United States of America	add to cart
Norco / hydrocodone 10mg Watson brand	฿3.35	vicodin(100)	United States of America	add to cart
1/4 g PURE AFGHAN HEROIN	฿15.78	tony76(99)	Canada	add to cart
1 GRAM - !EXTREMELY RARE! - PURE AFGHAN #4 HEROIN	฿50.30	tony76(99)	Canada	add to cart
1/2g PURE AFGHAN HEROIN - HIGHEST QUALITY	฿26.63	tony76(99)	Canada	add to cart
HEROIN (AFGHAN) 1/2 GRAM STR8 OFF KG-1/2 GRAM	฿30.70	W007(97)	Canada	add to cart
HEROIN (AFGHAN) PURE STRAIGHT OFF OF KG-1/4 GRAM	฿17.61	W007(97)	Canada	add to cart
1 g PURE AFGHAN HEROIN - HIGHEST QUALITY	฿41.42	tony76(99)	Canada	add to cart
.5g PharmerJohn's High Quality Black Tar Heroin	฿17.27	PharmerJohn(100)	United States of America	add to cart
1G**AFGHAN BROWN HEROIN **	฿20.67	Noriega(99)	Netherlands	add to cart
OxyContin 10 mg, 7x pills (70 mg total)	฿14.79	theOCguy(100)	France	add to cart
20g opium tea (dried & crushed natural poppy pods)	฿6.37	AlterEgo(99)	Austria	add to cart

Postaya Elle Konulan Küçük Paket veya Mektup Boyutundaki Uyuşturucu Miktarları

3.5 grams crystal meth

1.75 grams tar heroin

LSD blotter paper

1 gram cocaine

Posta İşletmecileri İçin Çeşitli Riskler Vardır:

- Başlıca endişeler
  - ✓ Posta markasının bütünlüğü
  - ✓ Çalışanların güvenliği: uyuşturucuya bağlı şiddet suçlarından kaçınmak
- Artan endişe

✓ Posta işleme sırasında posta çalışanlarının potansiyel olarak ölümcül kimyasallara maruz kalmaları

Ölümcül Doz: Eroin vs Fentanil

Fentanyl is a powerful synthetic opioid

Carfentanil: The equivalent of one grain of salt—ingested, inhaled, or absorbed through the skin—is enough to kill a person

- Posta akışında sıvı metamfetamin çıkabilir
  - ✓ elma suyu gibi gizlenmiş olabilir
  - ✓ çok tehlikeli
  - ✓ PCP, LSD ve diğer toksik sıvılardan kaynaklanan benzer risklere sahip

Zehirli Yasadışı İlaçlar, Zararlı ve Tehlikeli Maddelere Maruz Kalan İşletmeciler;

- Tehlikeli madde müdahale planları hazırlamalıdır
- Çalışan eğitimi ve farkındalığını arttırmalıdır.
- Kişisel koruyucu ekipman bulundurulmalıdır.
- Yerinde tıbbi ihtiyaçlar göz önünde bulundurulmalıdır.

Auto-inject antidote for opioid exposure

EKLER Uyuşturucu Madde ↓

Gizleme Yöntemleri

- Elektronik
- Gıda maddeleri
- Tüketici ürünleri
- Mumlar
- Heykeller ve antikalar
- Giyim
- Kumaş ve tekstil (ıslatma yöntemi)
- Çocuk oyuncağı
- Şeker
- Hediye paketi yapılmış hediyeler

EKLER Gizleme Metotları ↓

Yasadışı İlaçları Ele Alma Yöntemleri

Eğitim: Gişe memurları ve taşıyıcıları narkotik kaçakçılığı göstergelerinin farkında olmalı

Engelleme: Ulusal makamlarla işbirliği içinde uyuşturucuların ve ondan kaynaklanan para trafiğinin posta akışından çıkarılması

Sorumluluk: Ulusal makamlar ve diğer makamlarla ortak çalışma

Önleme: Farkındalık ve kamu hizmeti duyuruları; markayı korumak

Modül 5: Yasaklı Malların Postalanması Kara Para Aklanması

Kara Para Aklama Nedir?

Bu alt modülün sonunda aşağıdaki hususlar açıklanıyor olacak;

- Kara para aklama tanımı
- Kara para aklamanın aşamaları
- Yasadışı faaliyet türleri
- Mevcut gizlenme eğilimleri
- Postanın kara para aklama için nasıl kullanıldığı
- Kara para aklamaya karşı önlemler

Kara Para Aklama Nedir?

- Suçlular ya da suç örgütleri tarafından gelirlerinin yasadışı doğasını gizlemek için bu gelirleri meşru ticaret ve finans akışına sokarak kullandıkları süreç
- Kara para aklama, yasadışı gelir getiren çoğu suç faaliyetinde bulunur.

Kara Para Aklama İle İlgili Yasa Dışı Faaliyetler

- Fikri mülkiyet hakkı (FMH) ihlalleri
- Yasadışı ilaçlar
- Uyuşturucu kaçakçılığı
- Sigara kaçakçılığı
- Ateşli silah kaçakçılığı
- Posta sahtekarlığı (piyango postası)

Kara Para Aklama Aşamaları

Yerleştirme: büyük miktarlarda nakit parayı parasal araçlara dönüştürme (yani posta parası siparişleri)

Katmanlama: Bir dizi finansal işlemle kaçak gelirleri yasadışı kaynaklarından ayırmak

Entegrasyon: Paralar bir işletmeye, hisse senetlerine vb. yatırılır ve bir işletmenin iddia edilen kazancıyla elde edildiği görünümü verilir.

Gizlemenin Güncel Eğilimleri

Şüpheliler meşru görünmek için iş adlarını sıklıkla kullanır

Televizyonlarda, mikrodalga fırınlarda, elektrikli süpürgelerde veya diğer dayanıklı tüketim mallarında gizlenen nakit paralar

Küçük nakitler çoklu parsellere bölünür ve farklı adreslere postalanır

Posta Yoluyla Kara Para Aklama

- Toplu nakit veya finansal araçlar parsel halinde posta yoluyla gönderilir
- Saklanan değerli kartlar
- Posta havaleleri
- UPU Uluslararası Finansal Sistemi
- Elektronik transfer hizmeti

Kara Para Aklama İle Mücadele Araçları

- Şüpheli işlem bildirimi
- Dış kaynaklı finansal kuruluşların kendi kendine başlattığı denetimler
- Ulusal bankacılık yasalarına ve düzenlemelerine uygunluk
- Uluslararası finansal sistemin eğitimi

Yasadışı Ateşli Silahlar Trafiği Nedir?

- Yasadışı silah ticareti nedir ve postayı nasıl etkiler?
- Tipik gizleme yöntemleri
- Gönderiyi korumaya yönelik çözümler
- Meşru ateşli silahların uygunluğunu anlama

Yasadışı Silah Kaçakçılığı Nedir?

- Yasadışı silahlar kaçak silah, parça veya mühimmat kaçakçılığı veya yasadışı ticaretidir.
- Genellikle sınır ötesi faaliyet içerir
- Ateşli silahlarda yasal ticareti oluşturan şey, ülkenin yerel ve ulusal yasalarına bağlı olarak büyük ölçüde değişir.

Tipik Gizleme Yöntemleri

- Koliler
- Bilgisayarlar
- Ev Aletleri
- Bileşenlere demonte
- Diğer tüketim ürünleri

Postaya Etkisi

- Kolilerin tesliminde çalışanların risk içinde olması
- Mühimmat tehlikeli bir maddedir (patlayıcı)
- Posta işletmecisi uluslararası ve ulusal yasaların ihlallerinden sorumlu tutulabilir

Gönderiyi Koruma Araçları

Eğitim: Çalışanlar emarelerin farkında olmalı ve şüpheli maddeleri nasıl bildireceklerini bilmeli

Engelleme: Ulusal makamlarla işbirliği yaparak yasadışı silahları postadan çıkarmak

İrtibat: Kolluk kuvvetleri, makamlar ve diğer ilgili ulusal makamlarla işbirliği yapılması

Önleme: Eğitim ve posta kamuoyunun farkındalığı

Ateşli Silahların Postalanabilirliği

- AB'deki gibi birçok ülke için, tabanca, altıpatlar ve diğer ateşli silahları göndermek yasaktır.
- Pek çok ülke ateşli silah parçalarını ve ateşli silahlara benzeyen ögeleri yasaklar
- Ateşli silahların postalanabilirliği UPU Ülke Kısıtlaması'nda listelenmiştir
- 192 üye ülkenin
    - ✓ % 50'sinde yasak (izin verilmiyor)
    - ✓ % 35'inde postalanabilir
    - ✓ % 9'unda sınırlı (lisanslı, yetkili kurumlara)
    - ✓ % 5'inden hiçbir veri gelmedi

EKLER UPU Ateşli Silahlar Haritası ↓

Modül 5: Yasaklı Malların Postalanmasının Kötüye Kullanımı

Piyango Posta

Bu alt modülün bitiminde aşağıdaki hususlar açıklanıyor olacak;

- Kitlesel pazarlama dolandırıcılığını anlama
- Yasadışı piyango postasını belirleme
- Piyango postasının posta tüketicileri üzerindeki etkisini tanımlama
- Piyango posta yasağını açıklama

Kitle Pazarlama Dolandırıcılığı Nedir?

- Piyango posta toplu pazarlama dolandırıcılığı nedir? Telefon, mail vb. kullanarak kitle iletişim araçlarını kullanan sahtekarlıklar
- "Bu kazanan bir bilet, ancak talep etmek için paraya ihtiyacım var. Peşin para ile bana yardım edersen, ikramiyeyi seninle paylaşacağım. "

Sorunun Boyutu

- Gerçek mağdurlar mağdur olduğunu bildirmekte isteksiz olduğu için kitlesel pazarlama sahtekarlığı ile ilgili gerçek kayıplar tam olarak bilinemiyor.
- Küresel, kitle pazarlama sahtekarlığı zararlarının büyüklüğünün, milyarlarca dolarlık olduğuna dair güçlü göstergeler vardır.

En Yaygın Beş Sahtekarlık

- Kimlik hırsızlığı
- Borç toplama
- Banka ve borç veren
- Evde alışveriş
- Bahisler ve çekilişler

Yasadışı Piyango Postası Nedir?

- Nakit müşterilerine mail yoluyla dolandırıcı posta göndermek
- "Tebrikler! 400.000 $ 'a kadar ABD CASHI onaylı bir çek alabilirsiniz! Bir toplu ödeme! Vergisiz! WIN'e oranınız 1-6."
- "Her hafta gizli sistemimizi kullanarak yüzlerce kişi kazanıyor! İstediğiniz kadar kazanabilirsiniz!"

EKLER Yasadışı Bahis ↓

Piyango Postasının Posta Tüketicileri Üzerindeki Etkileri

- Depresyon
- Birikimlerin kaybı
- İntihar
- Limiti dolmuş kredi kartları
- Mülkiyet kaybı
- Evsiz kalmak

Piyango Postalarına Müdahale

Yasadışı İlaçlar

Bu alt modülün sonunda aşağıdaki hususları açıklıyor olacağız;

- Yasadışı ilaçlar nelerdir?
- Sorunun tehlikeleri ve kapsamı
- İnternet üzerinden ilaç satın almanın riskleri
- INTERPOL'un sorumluluğu

Yasadışı İlaçlar Nedir?

- Yasadışı hileli ilaçlar, sahte bir şekilde üretilmiş veya yanlış etiketlenmiş ilaçlardır.
- Sahte haplar gerçek muadilleriyle aynı görünebilir, ancak standart dışı koşullarda yanlış formüle edilebilir ve üretilebilirler.
- Yasadışı ilaçlar sıklıkla yanlış miktarda etken bileşen içerir veya hiç etken maddeleri yoktur.

Yasadışı İlaçlar Niçin Yapılır?

- İlaç sahtecileri diğer suçlularla aynı oranda dikkate alınmamıştır.
- Kolay para, sahtekarlar için en önemli motivasyondur.
- Üretim maliyetleri çok düşüktür.
- Kalite ve güvenlik standartlarına uyulmamaktadır.

Güncel Eğilimler

- INTERPOL üyesi ülkeler, ilaç suçuna karışan suçluların gayrı resmi ağlar üzerinden faaliyet gösterdiğini bildirmektedir.
- Dünya genelindeki geleneksel organize suç grupları, tedarik zincirinde ilaç suçuna da bulaşmaktadır.

- Bazı üye ülkeler, özellikle Güney ve Orta Amerika'da, son beş yılda ilaç suçlarında bir artış olduğunu bildirmiştir.
- Hem gayrı resmi ağlar hem de organize suç grupları aynı tür yasadışı ilaçlarda ticaret yapıyor görünmektedir: ağrı ve endişe giderici ilaçların yanı sıra ereksiyon bozukluğu ilacı; zayıflama hapları
- Birçok üye ülkede görülen eğilim, hem gayri resmi ağlar hem de organize suç grupları tarafından işletilen yasadışı çevrimiçi eczanelerin kullanımının artmasıdır.
- Bu uluslararası suç işletmelerine çok miktarda para akmıştır: ABD yetkilileri tarafından 2011 yılında ortaya çıkarılan yasa dışı çevrimiçi bir eczane ağı, iki yıl boyunca 55 milyon ABD doları kazanmayı başarmıştır.
- Kara para aklama, fuhuş ağları ve silah kaçakçılığı gibi diğer suçlar da ilaç kaçakçılığı işiyle ilintilidir.

Hızlı Posta İle İlaç Kaçakçılığı Halk Sağlığı İçin Büyük Bir Tehdit

- İlaç suçu; sahte, çalınmış yasadışı ilaçların ve tıbbi cihazların imalatı, ticareti ve dağıtımını içerir.
- Hırsızlık, dolandırıcılık, yasadışı oyun, kaçakçılık, insan ticareti, tıbbi ürünlerin yasa dışı ticareti ve kara para aklama suçlarıyla ilişkilidir.
- Sahte ilaçları ithal etmek için en sık kullanılan yöntem ekspres posta hizmetleridir.
- Sahte, çalıntı ve yasal ilaçların ve tıbbi cihazların imalatı, ticareti ve dağıtımında önemli bir artış vardır. Tüm dünyadaki hastalar sahte ilaçları ya da kötü saklanmış, içeriği ile oynanmış veya süresi dolmuş orijinal ilaçları bilmeden tüketerek sağlıklarını, hatta yaşamlarını tehlikeye atarlar.
- Yasadışı ilaçlar yanlış dozda aktif bileşen veya farklı bir bileşen içerebilir ya da hiç bileşen içermeyebilir. Bunlar bir dizi tehlikeyle ilişkilidir ve en kötü ihtimalle kalp krizi, koma veya ölümle sonuçlanabilir.
- Sahte ilaçlarla mücadele, ürünlerin dolaşım kalitesini sağlamak ve halk sağlığını küresel ölçekte korumak için çok önemlidir.
- Sahte ve yasadışı malların artan yaygınlığı, kolay, ucuz ve reçetesiz satın alınabilecekleri internet ticaretindeki artışla daha da artmıştır. Sorunun kapsamını belirlemek imkansızdır, ancak bazı Asya, Afrika ve Latin Amerika bölgelerinde sahte tıbbi ürünler pazarın % 30'una kadar çıkabilmektedir.

Sahte Tıbbi Ürünlerin Tehlikeleri

- Sahte ürünler zararlıdır ve hatta ölümcül olabilir.
- Sahte ilaçlar işe yaramaz veya oldukça tehlikeli olabilir.
- Fare zehiri gibi yüksek derecede toksik maddeler içerebilir.
- Sahte ilacı alan kişi, sağlıklarını tehlikeye atar.

Sorunun Kapsamı

- Sahte ilaç artık gerçekten küresel bir sorundur ve dünyanın bütün ülkeleri kaynak, transit veya varış noktaları olarak etkilenmektedir.
- Dünya Sağlık Örgütü (WHO) gelişmiş ülkelerde bulunan ilaçların yüzde 1'inin sahte olabileceğini tahmin ediyor. Bu rakam küresel olarak yüzde 10'a yükseliyor, ancak Asya, Afrika ve Latin Amerika'nın bazı bölgelerinde sahte ürünler pazarın yüzde 30'una kadar çıkabiliyor.
- Sahtecilik sadece ereksiyon bozukluğu ve kilo verme ilaçları dahil olmak üzere "yaşam tarzı" ilaçlar için değil, aynı zamanda kanseri, kalp hastalığını ve diğer ciddi hastalıkları tedavi etmek için kullanılanlar dahil olmak üzere hayat kurtarıcı ilaçlara da uygulanıyor.
- Sahte tıbbi cihazlar da risklidir. 'Tıbbi cihaz' terimi, kontakt lenslerden kondomlara kadar çok çeşitli sağlık bakım ürünlerini kapsar; cerrahi aletlerden şırıngalar ve radyoterapi makineleri ve tekerlekli sandelyelere kadar geniş bir yelpazede değerlendirilebilir.
- Giderek daha fazla insan, çevrimiçi eczaneler ve açık artırma siteleri aracılığıyla İnternet üzerinden ilaç ve tıbbi cihaz satın alıyor.
- Bu internet sitelerinin birçoğu yasadışıdır ve düzenlenmemiştir. Bu sitelerde yasadışı veya standart dışı ürünlerin ticareti yapılmaktadır.
- WHO, bu tür web sitelerinde bulunan ilaçların yüzde 50'sinin sahte olduğunu tahmin etmektedir.
- Çevrimiçi ilaçlar daha ucuz, daha hızlı ve daha uygun görünebilir, ancak tehlikeleri faydalardan çok daha ağır basar.
- Bu suçların arkasındaki suçluları tespit etmek, soruşturmak ve kovuşturmak için uluslararası düzeyde eşgüdümlü ve sektörler arası işlemler hayati öneme sahiptir.

INTERPOL'un Sorumluluğu

INTERPOL bu ana sorunu üç ana yolla ele almaktadır:

- Uluslararası suç ağlarını bozacak sahadaki operasyonları koordine etmek.
- İlaç suçu ile mücadelede yer alan tüm kurumların bilgi ve becerilerini geliştirmek için eğitim vermek.
- Çeşitli sektörlerde ortaklıklar kurmak.

Interception of anti-malarial medicines by Togo Customs

5,000 units of counterfeit medicines in air-filter machines

EKLER Yasadışı Eczacılık Ürünleri İçeren Posta Kalemleri ↓

Yasaklı Malların Postalanmasının Kötüye Kullanımı - Fikri Mülkiyet Hakkı (FMH)

Hedefler

Bu alt modülün sonunda aşağıdaki hususları açıklanıyor olacak:

- Fikri Mülkiyet Hakkı nedir?
- Patentler, ticari markalar, telif hakları ve ticari sırlar nelerdir?
- Fikri mülkiyet neden önemlidir?
- Sahte ürünler nelerdir?
- Tehdit nedir?

Fikri Mülkiyet Nedir?

- Fikri mülkiyet, aklın ve insan zakasının bir ürünüdür.
- Bu ürünler, “fikir icatları ve kreasyonları” olarak ticari değere sahiptir

Fikri Mülkiyet Otoriteler Tarafından Korunmaktadır:

Patentler, Ticari Markalar, Telif Hakları ve Ticari Sırlar

- **Patent;** Buluş sahibine, buluşlarını sınırlı bir süre için özel olarak kullanma hakkı verir. (20 yıl)
- **Ticari Markalar;** Bir şirketin ürünlerini tanımlamak için kullandığı benzersiz isim, logo, sembol, tasarım ve renkleri korur.
- **Telif Hakları;** yaratıcı sanatsal ifadeleri korur
- **Ticari Sırlar;** Bilgiyi korumak için makul önlemlerin alındığı ve işletmeci tarafından bağımsız bir ekonomik değer taşımasından dolayı açıklanmayan gizli olan bilgileri kapsar.

Ticari Marka Türü

Olağandışı Markalar

Telif Hakkı

- **Orijinal Eserleri Korur**
  - Edebi, dramatik, müzikal, sinema filmi, ses kayıtları, sanatsal eserler
- **Koruma**
  - Oluşturulduktan sonra otomatik olarak güvendedir.
  - Yazarın hayatını içeren dönem +70 Yıl.
  - Eğer yazar tüzel kişilikse yayından 95 yıl veya yaratımından 120 yıl.
- **Kriterler**
  - Orijinal olmalı
  - Somut bir ifade aracılığıyla ifade edilebilmeli
  - Yaratıcılık olmalı.
- **Fikri Mülkiyet Hakları (IPR) Merkezi**

1999 yılında iki ajansla, ABD Gümrükleri ve FBI ile başladı. 2008'de IPR Merkezi, ICE (Immigration and Customs Enforcement- Göçmenlik ve Gümrük Muhafaza), CBP (Customs and Border Protection- Gümrük ve Sınır Koruma Birimi) FBI, USPIS (The United States Postal Inspection Service-Amerika Birleşik Devletleri Posta Müfettişliği), FDA (Food and Drug Administration-Gıda ve İlaç Kurumu) ve DOC (Department of Commerce- Amerika Birleşik Devletleri Ticaret Bakanlığı) ile güçlendirildi. Bugün IPR Merkezi, 23 federal ve uluslararası kuruluşun ortaklaşa çalıştığı bir örgüttür.

Neden Fikri Mülkiyet?

Sahte Ürün Nedir?

- Meşru bir malın hileli taklidi

Sahte Ürünlerin Etkileri Nelerdir?

- Sağlık ve güvenlik riskleri
- Ekonomik sonuçlar
- Organize suç finansmanı
- Dolandırıcılık ve Kötüye Kullanma
- Sahtecilik ve korsanlık, ABD ekonomisine yılda 200 ila 250 milyar Dolarlık bir maliyete neden olmakta.
- Sahte ürünlerin dağıtımı, Amerika Birleşik Devletleri'nde bir suçtur ve ciddi fiziki yaralanma veya ölüm meydana gelirse, cezai yaptırım veya ömür boyu hapis cezası ile cezalandırılır.

Fikri Mülkiyet Soruşturması

Başarılı bir posta soruşturması için dört temel unsur:

1. Gümrükten alınan bilgiler
2. İyi soruşturma ve kovuşturma iyi kanıtlarla gerçekleşir
3. Başından beri yargı organlarıyla ile çalışmak
4. Baştan itibaren hak sahibi ile çalışmak.

Çoğu fikri mülkiyet soruşturması aşağıdaki yöntemlerle yürütülür:

- Gümrük ve sınır koruma
  - ✓ Risk analizi
  - ✓ El koyma
- Sanayi - Hak sahibi
  - ✓ Suç içerikli web siteleri (Rogue Websites)
  - ✓ Lokasyonlar
- Bilgi kaynakları
  - ✓ Kamu
  - ✓ Diğer suçlular

EKLER Yasadışı Eczacılık Ürünleri İçeren Posta Kalemleri ↓

Modül 5: Yasaklanan Malların Kötüye Kullanımı - Yasadışı Sigara Kaçakçılığı

Hedefler

Bu alt modülün sonunda aşağıdaki hususlar açıklanıyor olacak:

- Yasadışı sigara kaçakçılığı nedir ve neden ortaya çıkar?
- Kaçakçıların kullandığı yöntem ve stratejiler
- Küresel kaçakçılık eğilimleri
- Sahte sigaraların sağlığa etkileri
- Sigara kaçakçılığı davaları

Yasadışı Sigara Ticareti Nedir?

- Yasadışı sigara ticareti, “mevzuata uymayan üretim, ithalat, ihracat, satın alma, satış işlemlerine tabi tutulması” olarak tanımlanmaktadır.

- Yasadışı sigara ticareti faaliyetleri 3 kategoriye ayrılır:
- **Kaçak:** yurtiçi vergi ödemesi olmadan yurtdışından getirilen sigaralar
- **Sahte:** tüketicileri aldatmak ve vergi ödemekten kaçınmak amacıyla hak sahiplerinin izni olmadan üretilen sigaralar
- **Yasadışı Beyazlar:** başka bir ülkede yasal olarak üretilmiş, ancak vergileri ödenmeden başka bir ülkeye kaçırılmış ve satılmış ürünler

Yasadışı Sigara Ticaret Trafiği Nedir?

- Yasadışı sigara ticareti, satış ve tüketim için sigaraların düşük vergilendirmeli bir idari bölgeden yüksek vergilendirmeli bir bölgeye taşınmasıdır.

Yasadışı Sigara Ticareti Neden Ortaya Çıkıyor?

- Vergiden kaçınma yoluyla büyük kârlar elde etme
- Tüccarların ve tüketicilerin fazla talebi
- Tüketicilerin, tütün vergilerini azaltarak tasarruf etmek istemesi
- Tedarikçilerin kolay sınır girişinden, yüksek kâr marjlarından ve eğer yakalanırsa hafif yaptırımlardan yararlanmak istemesi

Fotoğraf Litvanya Gümrüklerine Aittir

Photo courtesy of Lithuanian Customs

Illegal production of cigarettes

Kaçakçıların Kullandığı Yöntem ve Stratejiler

- Normal üretim ve dağıtım kanalları boyunca her noktada sigara ticareti gerçekleşebilir
- Normal ticari akışların dışına ve karaborsaya yönlendirilir
- Üreticiler "kayıt dışı" sigaralar üretebilir ve üzerlerindeki vergileri ödemezler
- Perakendeciler sigaralarının bir kısmını veya tamamını "el altından" satabilir ve böylece satış vergisi ödemesini önleyebilir

- Bireyler, perakende satış veya toptan satış düzeyinde, bir alanda büyük miktarlarda sigara satın alabilir ve daha sonra, bazen "smurfing (kara para aklama sırasında tespit edilmeme amacıyla aklanan meblağı küçük hesaplara bölerek kaçırma)" olarak adlandırılan bir işlemle, başka bir alana veya ülkeye taşıyabilir

Küresel Kaçakçılık Eğilimleri

	2012 Number of Quantity	2013 Number of Quantity
Cigarettes Seizure	5,574	6,564
Cigarettes Pieces	2,568,583,011	2,703,823,441

An emerging trend that is worth pointing out is the appearance of "mail" as a new concealment method for large quantities. In 2012 this method was not observed while in 2013 it was observed twice.

Yasadışı/Sahte Sigaraların Sağlığa Etkileri

- Sahte sigaraların içeriği, orijinallerinden büyük ölçüde farklı olacaktır.
- Sahte sigara üretiminde, kalite kontrolü çok az veya hiç yoktur.
- Sahte sigaralar, tehlikeli, zehirli metal seviyeleri de dahil olmak üzere, endişe verici derecede yüksek kirleticilik seviyelerine sahiptir
- Sahte sigaralar ciddi bir halk sağlığı riski oluşturur
- Gençlerin sigara içme oranını arttırır

Sigara Kaçakçılığı Davaları: Sahte Dev Jin Ling

Bu ürün Doğu Avrupa ve Rusya'ya yayılmakta ve ürünleri Avrupa Birliği'ne giriş yapmaktadır. Yılda en az 1 milyar dolar değerinde olan ticaret sadece bir markayı içeriyor: Jin Ling, Camel'e benzeyen bir ambalajı olan Jin Ling'in yasal bir pazarı yoktur ve reklam yapmamaktadır.

Sigara Kaçakçılığı Davaları: Sahte Dev Jin Ling

- Çinliler, 1990'ların sonlarında üst düzey Batı sigara markalarının paketlerinin üzerindeki koruyucu hologramları çoğaltan teknolojiyi kullanmaya başladıklarında, bir tütün sahteciliği devi doğmuştur.
- Bugün Çin, yılda yaklaşık 200 milyar adet ile en büyük sahte sigara üreticisi haline gelmiştir.
- Çin malı Marlboro, Newport ve diğer markalarla yüklenen gemiler; çiniler, oyuncaklar ve mobilyalar olarak gizlenen gönderilerde dünya çapındaki limanlara giriş yapmaktadır.

Sahte Sigara İçeren Posta Öğelerini Tanımlama

- ÇIKIŞ VE VARIŞ ÜLKELERİ
- İÇERİĞİN TANIMI
- SARGILAR
- GÖNDERENİN İSMİ VE ADRESİ
- AĞIRLIK TUTARSIZLIĞI
- BÜYÜKLÜK VE BİÇİM

Posta Yoluyla Yasadışı Sigaralar

Modül 6: Dâhili ve Harici Posta Hırsızlığı - Dâhili Posta Hırsızlığı

Modülün sonunda aşağıdaki hususlar açıklanıyor olacak:

- Posta hırsızlığı olayını belirleme yöntemleri
- Potansiyel şüphelileri belirleme teknikleri
- Bütünlük testi teknikleri

Dâhili Posta Hırsızlığı

- Çalışanlar, yükleniciler ve posta sistemine iç erişimi olan diğerlerinin posta hırsızlığı
- Çalışanlar
- Ulaştırma servisleri
    - ✓ Havayolu çalışanları
    - ✓ Yer hizmetleri personeli
    - ✓ Nakliyecilik/Teslimat yüklenicileri
- İşleri nedeni ile postaya erişimi olan diğer kişiler

- Dâhili hırsızlığı belirleme ve önleme yöntemleri
    - ✓ Güvenlik ve önleme
    - ✓ Kayıp verilerinin derlenmesi ve analizi
    - ✓ Çalışanların ve yüklenicilerin soruşturulması
    - ✓ Teşhis ve tutuklama (mümkünse cezai kovuş-turma)
    - ✓ Başarılı soruşturmaların duyurulması

İç Hırsızlık Çeşitleri

- Kıymetli postaların çalınması
  - ✓ Para
  - ✓ Mücevher
  - ✓ Finansal araçlar
  - ✓ Kredi kartları
  - ✓ Elektronik
- Kişisel kullanıma bağlı devam eden sistematik hırsızlık
  - ✓ Finansal zorluk
  - ✓ Kumar
  - ✓ Uyuşturucu/Alkol Bağımlılığı
  - ✓ Açgözlülük
  - ✓ Heves için hırsızlık
  - ✓ Kötü muameleyi telafi etmek için hırsızlık
- Büyük çaplı organize hırsızlık
  - ✓ Kredi kartları
  - ✓ Yüksek değerli ürünler
- Postalardan çalınan kişisel kimlik bilgileri ile finansal dolandırıcılık girişimi
  - ✓ Kimlik dokümanları
  - ✓ Önceden onaylanan kredi teklifleri

Gizli Hırsızlıklar

- Dikkatleri dağıtmak için bazı çalışanlar, çalışma arkadaşlarının kontrol bölgelerinden posta ve diğer değerli eşyaları çalma fırsatını gözlüyor.

Yıkım veya Anlaşmazlık Nedeniyle Hırsızlık

- Teslimat personeli tarafından
  - ✓ Teslimat alanının bölümleri için bütün postalar olabilir
  - ✓ İş yükünü azaltmak için belirli posta türleri olabilir
- Taşıma personeli tarafından yüklerini hafifletmek
  - ✓ Kamyon
  - ✓ Demiryolu
  - ✓ Hava transferi

Hırsızlık Bileşenleri

- Erişim
- Fırsat
- Motivasyon
- Gizleme

Şüphelileri belirlemek için hangi çalışanların bu dört bileşenin hepsine sahip olduğunu düşünün?

Güvenlik ve Önlem

- Posta çalışanları postaların dokunulmazlığı konusunda eğitilmeli ve olası sonuçları konusunda uyarılmalıdır.
- Cezalar halka açık şekilde yayınlanır.
- Açık denetleme yöntemi caydırıcı olarak kullanılır.

Kayıp Verilerin Derlenmesi ve Analizi

- **Kaynaklar**
  - ✓ Kayıp postaların, eksik içeriklerin kurcalanması ya da finansal suçlara yönelik müşteri şikâyetleri
  - ✓ Büyük oranlı posta kayıp raporlarına ilişkin ipuçları
  - ✓ Açılmış posta raporları
  - ✓ Taranmış ama teslim edilmemiş postaların kaybolması

- **En İyi Uygulamalar**
  - ✓ Bilgisayar veri merkezindeki kayıp verilerin istatistiki analiz için derlenmesi
    - Yüksek kayıp oranına sahip özel tesisleri tespit etmek
    - Yüksek kayıp oranına sahip transfer rotalarını tespit etmek
- **Olası Şüpheleri Tespit Etmek İçin Kayıp Veriler İle Geçmiş Çalışan Takvimlerini Kıyaslamak**

Grafik Örneği

- 13-17-21 ve 24 Aralık tarihlerinde posta ofisinin çöp kutusunda bulunan açılmış postalar
- O tarihlerde saptanmış bütün çalışanlar

	Dec 13	Dec 17	Dec 21	Dec 24
Employee A	✓	✗	✗	✓
Employee B	✗	✓	✓	✗
Employee C	✓	✓	✓	✓

Çalışanların Soruşturulması

- Şüphelenilen hırsızların teftişi
- Doğruluk testi
- Finansal soruşturma
- Kabul edilen diğer soruşturma metotları

Doğruluk Testi

Kör Test (Blind Test)

- Kıymetli postalar kaybın oluştuğu bölgeye gönderilecek veya yerleştirilecek, ya da doğrudan şüpheliler bu işlem veya teslimatla karşılaşacak
- Postalar kayıpları tespit etmek için kopyalanır
- Kontrol altındaki teslim noktasına gönderilir
- Ya da var olmayan bir adres gönderinin üzerine yazılır
- Farklı bir adreste teslimatı önlemek için çok alışılmadık bir isim kullanılır
- Eğer posta kaybolursa, nerede ve nasıl kaybolduğu bilinir
- Etkili kör testleri genellikle hırsızlıkla ilişkilendirilebilecek veriler içerir

Canlı Test (Live Testing)

Bir şüpheli tespit edildiğinde, soruşturmayı yapan kişi "Canlı Test" yaparak bir postayı veya koliyi yem olarak kullanabilir.

- Çalınmasını beklediğini bir gönderi hazırlayın
- Kaybolduğu bilinen gönderiye benzer bir mektup veya koli oluşturun
- Gönderiyi belirgin bir şekilde tespit edecek şekilde fotoğraf yada başka bir şekilde belgeleyin

Posta müfettiş şefi J. Holbrook'un 1855 tarihli "Posta Çantasında 10 yıl" isimli kitabından:

> It is very clear that decoy letters can never injure honest men. These missives trouble no one who does not unlawfully meddle with them, and it can hardly be claimed that they offer any greater temptations to the dishonestly inclined than any other class of money-letters. It is of course impossible for any one to distinguish between a decoy letter and a genuine one, and he who faithfully discharges his duties in reference to other letters, will never find out by his own personal experience, that there are such things as decoys.

- Test postası şüpheli tarafından görünebilecek şekilde yerleştirilmelidir
- Posta gönderi süresince elektronik ortam üzerinden veya doğrudan gözetlenmelidir
- Video kaydı yapılması hukuki süreç açısından değerli olacaktır

Canlı Test ve Yakalama

- Test postası şüpheli tarafında çalındığında konu ile alakalı yetkili kuruluş ile işbirliği yapılmalıdır
- Şüpheli, yetkili tarafından yakalanıp olay yerinde uzaklaştırılmalıdır
- Yakalanan şüpheli sorgulanmalı ve soygun ile alakalı ilave bilgiler ve itiraf (gerekli değil ama tercih edilir) alınmalıdır,
- Soyguncunun kişisel dolabı, odası ve arabası olası diğer kayıp postaları bulmak üzere aranmalıdır
- Soyguncuya diğer çalışanlardan hangilerinin hırsızlık yaptığı ile alakalı bilgiler alınmalıdır

Ceza, Kovuşturma ve Posta Yönetimi Rapor Hazırlanması

- Posta yönetimine bir rapor sunulmalıdır
    - ✓ Öncelikli olarak çalınan posta, soruşturma süreci, deliller ve çalışanın itirafı veya reddini barındırmalıdır
    - ✓ Eğer bir güvenlik açığı tespit edilmiş ise geliştirmeye yönelik tavsiyeler bulunmalıdır
- Soruşturmanın mevcut bütün belgelerinin yasal sorumluya ya da ceza savcısına teslim edilmesi
    - ✓ Çalışanın bilgilerini, hırsızlığın detaylarını, kurbanın mağduriyetini ve diğer bütün bilgileri içeren bir dosya hazırlanmalıdır
    - ✓ Mevcut ise fotoğraf ve videolar da sunulmalıdır

İç Tanıtım

- Gelecekteki hırsızlıkları önlemek adına çalışan eğitimlerinde eski soruşturmaların örnekleri gösterilmelidir
- Çalışanlara şüphelendikleri olayları raporlama yöntemleri gösterilmelidir
- Şüpheli durumların raporlanmasını teşvik amacıyla bir ödül sistemi düzenlenebilir

Bir postanın özellikle bir çalışan tarafından çalınmasını önlemek bir posta işletmecisinin en kritik sorumluluğudur.

Modül 6: Dâhili ve Harici Posta Hırsızlığı – Dış Etkenler

Harici Posta Hırsızlığı Konusunda Eğitim Verilmesi

- Hangi postaların çalındığını tespit etmeye yönelik yöntemler belirlenmesi
- Kaybolan ya da çalınan postaların değerlerinin tespiti için raporlanması
- Posta hırsızlığının yaşandığı bölgelerin tespit edilmesi için temel düzeyde bir soruşturma yönteminin bilinmesi
- Çalınan, kopyalanan ve sahte finansal dokümanların tespitinin yapılması
- Soruşturma süresince yasal yetkililere raporlama yapılması
- Harici posta hırsızlığı doğrudan postalara erişim yetkisi olmayan kişiler tarafından yapılmaktadır ve postanın teslim edileceği yere önceden giderek teslim alırlar
- Harici posta hırsızlığı soruşturma programının amacı:
    - ✓ Kullanıcılarının postalarının güvenliği ve korunması

✓ Posta işletmecisinin marka değerinin korunması

✓ Dâhili hırsızlığı veya karışıklığı önlemek amacıyla temel bir soruşturma yürütmek

- Posta düzenleyicileri tarafından soruşturmalara dikkat çekerken aynı zamanda yasal yaptırımlara yardımcı olmak özellikle çalınan postalar polis nezdinde birincil önem düzeyinde değilse
- Hırsızlık
- Kanuna aykırı zilyetlik
- Engelleme
- Uygunsuzluk
- Postaya zarar verme

Öncelikler

- Yüksek sayıda kayıplar

✓ Araba hırsızlığı

✓ Posta kutusu ve posta çantası hırsızlığı

✓ Posta depolarına ve posta kutularına saldırı

✓ Hane içleri posta kutularına yönelik hırsızlık

✓ Posta arabalarının ve depolarının anahtarlarının çalınması

✓ Posta tesislerinde hırsızlık

- Organize suçlar

✓ Yakalanmayı önlemek için belirli bölgelere yerleşilmesi

✓ Posta çalışanları ile iş birliği yapılması

Toplu Saldırılar: Tek Hırsızlık İle Birden Çok Müşteriye Etki Etme

- Yüksek sayıda postaya ulaşmak için posta arabalarına yönelik yapılan saldırılar

Posta Kutularından Çalmak

- Hedef posta kutusunu detaylı şekilde incelemek
- Yüksek hırsızlığın olduğu bölgelerde posta kutularına ekstra bir güvenlik önlemi alınması. (Yapışkan bir cisim ile birden fazla mektubu kutudan çıkarmak)
- Posta kutusunun etrafında veya postalarda yapışkan izleri olup olmadığı kontrol edilmeli

Kimlik Hırsızlığı

- Bir kişinin kredi kart numarası veya kimlik kartı gibi kişisel bilgilerinin kanunsuz yollar ile ele geçirilmesi
- Yaygın teknik
  - ✓ Mektup çalınır
  - ✓ Mektup içerisindeki kişisel bilgiler kredi kartına başvurmak için kullanılır
  - ✓ Kredi kartını kendi harcamaları için kullanırlar
- Kredi kartı hırsızlığı ayrı ayrı gönderilen kimlik bilgilerinin hırsızlığına da yol açabilir.

Sahte Çekler

- Alacaklı isimlerini ve alacak miktarlarını silmek için kimyasal maddeler kullanılır.
- Yeni alacaklı ve tutar çeke yazılır.
- Kredi kartı hırsızları, ayrı olarak gönderilen kişisel kimlik numaralarını (PIN) çalmak için iade edebilir.

Sahte Finansal Ekipmanlar

- Sahte çeklere benzer şekilde, sahtecilik posta hırsızlığı için de teşvik edici bir neden olabilir.
- Hesap numaraları ve yönlendirme bilgileri gibi banka bilgileri, çalınan çeklerden alınabilmekte ve yeni çeklerin oluşturulmasında kullanılabilmektedir.

Postaların Engellenmesi, Tahrif Edilmesi veya Gecikmesi

- Posta hırsızlığında olduğu gibi, müşteriler genellikle posta işletmecisini suçlayacaklardır.
- Kişisel sebepler (aile/komşu anlaşmazlıkları)
- İş rekabeti
- Vandallar
- İhmalkar üçüncü taraf posta işleticileri
    - ✓ Otel personeli
    - ✓ Gayrimenkul temsilcileri
    - ✓ Özel kuryeler

Posta Tesisi Hırsızlıkları

- Posta paketleri veya diğer varlıkları elde etmek için posta tesislerinin hedeflenmesi

Hırsızlık Önlemleri

- Fiziksel ve operasyonel güvenlik ekipmanı ve politikalarının uygulanmasını sağlamak için posta tesislerinin değerlendirmeleri yapılmalı.
- Şubeler, suçlu perspektifinden değerlendirilmeli. Birisi, postaya veya tesise izinsiz olarak nasıl erişebilir?
- Alarmlar, yüksek güvenlikli kilitler, video kameralar, aydınlatma vb. gibi hangi karşı önlemler geliştirilebilir?
- Çalışanların uygun güvenlik prosedürlerini takip ettiği doğrulanmalı. Kapıların kilidi açık mı? Posta güvenli bölgelerde saklanıyor mu? Çalışanlar uygun güvenlik uygulamalarından haberdar mı?
- Çalışanların usulsüzlükleri ile ilgili bir sorun mu? Bazı çalışanlar kasıtlı olarak harici suç ortaklarının postalara erişimine izin vermektedir.

Posta Hırsızlığını Araştırmak İçin Önce Bir Sorun Olduğunu Bilmeniz Gerekir

- Muhtemel hırsızlık raporlarını kabul etme sürecine sahip olun
    - ✓ Müşteri şikayetleri
    - ✓ Teslim edilmeyen ticari posta raporları
    - ✓ Son teslimat taraması olmadan yapılmış nakil halinde olan taramalar
- Hırsızlığın muhtemel konumlarını belirlemek için uyumlu verileri değerlendirin
- Öncelikli vakaları belirleyin (tek bir yerde yüksek hacimli ürünler veya birden fazla mağdur)
- Muhtemel hırsızlık yerindeki işlemleri gözlemleyin
    - ✓ Posta gözetimsiz ve teminatsız mı?
    - ✓ Birçok kişi tarafından erişilebilir mi?
    - ✓ Postaları veya çalınan içerikleri gizleme fırsatları

Yaygın Kayıp Önleme Yöntemleri

- Hırsızlık / kayıp raporlarının derlenmesi ve verilerin analizi
- Görüşmeler (mağdurlar, tanıklar ve belki de şüpheliler)
- Yüksek hacimli ticari postalardan gelen bilgilerin analizi
- Gözetim (canlı veya kaydedilmiş video aracılığıyla)
- Bilgi için ödüller
- Gizli çalışanların veya ücretli muhbirlerin kullanımı

- Hırsızlık olaylarının sık görüldüğü yerler üzerinden kasıtlı olarak geçen cazip öğeler
- İçeri gizlenmiş Konumlandırma Sistemi (GPS) vericileri
- Tuzak mektuplar kullanılan para değerli perakende hediye kartları

Video Kayıtlarının İncelenmesi

- Bu fotoğraflar, gizli video kameralardan ve müşterilerin eksik postalardan şikayet ettikleri ticari posta odalarından alınmıştır

Yasanın Yürütülmesine Yönlendirme

- Bazı posta işletmecileri, cezai uygulamanın ek bir caydırıcı unsur olduğunu düşünmektedir. Bu nedenle, polise veya ilgili diğer kanun uygulayıcı makamlara bir rapor sunmak yararlı olacaktır. Aşağıdaki bilgiler göz önünde bulundurulmalıdır:
    - ✓ Belirli bir posta hırsızlığı vakasının tam geçmişi
    - ✓ Mağdurlar ve suçun sonuçta ortaya çıkan etkisi
    - ✓ Tanıklar ve sağlayabilecekleri kanıtlar
    - ✓ Çalınan posta miktarı ve parasal değer
    - ✓ Mevcut kanıtların bir listesi (kurtarılan posta, video vb.)
    - ✓ Topluma ve posta işletmecisine etkisi
    - ✓ Kimlik hırsızlığı, dolandırıcılık, çalıntı mal satışı, vb. gibi posta hırsızlığına ek olarak işlenen posta dışı suçlar

EKLER

2.1 Güvenlik Riski Değerlendirme Matriksi

Sayfaya Geri Dön

Security Risk Assessment (EXAMPLE)

Security Risk Analysis **Appendix 1**

Threat factors	#	Threat scenarios, known and/or anticipated	Organization Vulnerability: Existing mitigation Fully Mitigated 1 Largely Mitigated 2 Partially Mitigated 3 Little mitigation 4 No Mitigation 5	Organization Vulnerability: Remaining vulnerabilities	Threat Likelihood Very Unlikely 1 Unlikely 2 Moderately Likely 3 Likely 4 Very likely 5	Simplicity/ Feasibility of Attack Very easy 5 Easy 4 Intermediate 3 Difficult 2 Very difficult 1	Threat Impact Negligible 1 Minor 2 Moderate 3 Severe 4 Critical 5		Risk level Very Low Low Medium High Very High	History threats	Risk level after mitigation	Risk Priority	Recommended Mitigating Measures
Violent Crime	1	Armed aggression with intent to kill employees.	Largely Mitigated 2 • Security Plan		Unlikely 2	Intermediate 3	Critical 5		Medium 10	No history	Low 5	13	
	2	Mail bombs/ IED	Largely Mitigated 2 Staff trained to observe suspicious items.		Moderately Likely 3	Easy 4	Critical 5		High 15	No history of real or hoax bomb	Medium 10	1	.
	3	Attack on individual: attack against specific individuals in offices and public spaces.	Partially mitigated 3: All visitors required to sign in. Staff is security trained.	Posts are open areas of commerce.	Moderately Likely 3	Intermediate 3	Negligible 1 Casualties' likely, somewhat reliable scenario.		Very Low 3	No history	Very Low 3	68	• Access control to all buildings • Access control to all sensitive offices .
	4	White powder incident	Largely mitigated 2:		Moderately Likely 3	Very difficult 1 Target individual, significant contaminations of others, biological agents are extremely difficult to source.	Severe 4 Casualties imminent, somewhat reliable scenario		High 12	Yes Only fake powder.	Medium 9	4	
	5	Bomb Threat	Largely mitigated 2	Fence perimeter not difficult to climb, not all cars searched.	Moderately Likely 3	Very Easy 5	Moderate 3		Medium 9	2 bomb threats Without disruption of activities.	Medium 9	19	
Disaster/ Weather Condition	6	Earthquake	Little mitigated 4 Evacuation exercises.		Very Unlikely 1	-	Severe 4		Low 4	Few earthquakes	Low 4	59	• Evacuation training Business Continuity Plan • Disaster Recovery Plan • Crisis Management Plan
	7	Fire	Partially mitigated 3	Lack of sprinkler	Very	Easy 4	Moderate 3		Very Low 3	No history	Very Low	68	

Security Risk Assessment (EXAMPLE)

			• Fire extinguisher • Upgrade of fire detection system (smoke and heat detectors) • Fire doors and control zones/partitioning under construction	system and building compartementation	Unlikely 1						3		• BCPBusiness Continuity Plan • Disaster Recovery Plan • Crisis Management Plan • Increase funding to install a full sprinkling system.
	8	Snow Storm	Largely mitigated 2 • Staff Stay at home		Unlikely 2	Intermediate 3	Minor 2		Low 4		Low 4	59	• Staff work from home • Business Continuity Plan • Disaster Recovery Plan • Crisis Management Plan
	9	Water floods from infiltration and rain.	Partially mitigated 3 Water pumps, archives removal,	Archives to be removed	Unlikely 2	na	Severe 4		Medium 8	Some basements flooded, archives flooded.	Low 4	27	• Repair, removal of important documents, water pump Business Continuity Plan Disaster Recovery Plan
Criminal/ External Attacks	10	Burglary	Largely mitigated 2 New intrusion detection system		Moderately Likely 3	Difficult 2	Minor 2		Low 6		Low 6	42	• Access control and physical security measures, security foot patrols. • Master key audit
	11	Litigation resulting from workplace injury.	Largely mitigated 2 All workplace injuries subject to reporting and investigation where appropriate.	na	Moderately Likely 3	Easy 4	Minor 2		Low 6	na	Low 6	42	na
	12	Vandalism.	Largely mitigated 2 New intrusion detection and CCTV system fully operational.	Impossible to monitor all visitors.	Moderately Likely 3	Easy 4	Negligible 1		Very Low 3	na	Very Low 3	68	
	13	Computer hacking, introduction of spy ware, subversive software, substantial sabotage to the IT system.	Largely mitigated 2	Impossible to obtain 100% computer security against professional hackers.	Unlikely 2	Intermediate 3	Severe 4		Medium 8	Na	Medium8	27	Train staff on the use of internet with maximum security. Software Encryption facilities for sensitive communications
	14	Theft by staff		Impossible to control	Moderately	Easy 4	Minor 2		Low 6		Low 6	42	

Security Risk Assessment (EXAMPLE)

			Largely mitigated 2	and monitor all staff behavior.	Likely 3								
	15	Misuse of computer system by staff	Largely mitigated 2	Impossible to obtain 100% computer security against professional hackers.	Moderately Likely 3	Intermediate 3	Moderate 3		Medium 9	No history	Medium 9	19	
	16	No UPS or power back up-system	Largely mitigated		Unlikely 2	Intermediate 3	Moderate 3		Low 6	No history	Negligible 3	42	Install a complete power backup system able to power

NOTE: Risks identified at Medium (9) and above have been identified as those risks which fall in to the category of risks which are deemed to be 'unacceptable' risk and require mitigation measures to reduce the risk to within an acceptable level.

2.2 Tesis Güvenlik Planı

Sayfaya Geri Dön

Section 1

Facility Access

1Facility Access

11 Referenced Documents:

If there are other documents used as references list the here.

12 Purpose

Provide a standard and consistent method in which access into Postal installations will be controlled.

13 Scope

Access to all workroom areas is limited to authorized on-duty postal employees and authorized contractors. All other individuals are excluded unless they have legitimate business on the floor and are properly escorted.

14 General Security Responsibility

All employees are charged with the responsibility of preventing unauthorized access by individuals, including off-duty employees, from entering restricted areas. All individuals on the workroom floor who are not properly identified or escorted should be immediately challenged.

15 Accountability Procedures

Installation heads are required to carefully evaluate the work-flow cycles of their units to determine when the workroom floor can be locked. This is normally at all times except during heavy traffic periods when employees are reporting to or departing from work. The policy governing the locking of doors should be firmly adhered to. Supervision to ensure compliance is necessary to afford maximum protection of postal employees, funds, and property. Emergency egress is to be provided in accordance with national and local rules and regulations.

Section 2

Facility Keys

2Facility Keys

21 Referenced Documents:

If there are other documents used as references list the here.

22 Purpose

Provide specific instructions for establishing and maintaining strict accountability and an accurate inventory of all Facility Keys assigned to a postal facility. Provide specific instructions for establishing proper protection under signature, receipt, assignment and accountability for each facility. These procedures are the minimum standards permitted and local management may provide a more stringent set of requirements.

23 Scope

Facility keys can include master keys, exterior entrance keys, special keys such as those for Registry Cages, vaults, stamp stock rooms, employee record rooms, etc. Personnel are issued only such keys, as their duties require. Entrance lock keys are furnished only to those postal employees who are required to open the office in the morning or close at night.

Master keys are issued to maintenance employees only during their tours of duty and may not be carried from the building. No other occupants of the building are issued master keys, and any such keys in the possession of other occupants must be recalled. Master keying is not permitted for locks opening stamped envelope rooms or other locations requiring individual accountability of contents. This applies to exterior doors in retail and delivery facilities.

24Responsibility

The **Installation Head** is responsible for ensuring a facility's compliance with established security procedures.

241Postal Service Keys and Access Control Cards

242.1 Postal Employees

Personnel are issued only such keys as their duties require. Entrance lock keys are furnished only to those postal employees who are required to open the office in the morning or close at night. Management reviews employee key requirements semi-annually. They are not on a master key system. Standard locks are not authorized on exterior doors or in high security areas.

242.2 Nonpostal Occupants

Nonpostal occupants may be furnished keys to the entrance door of their offices when necessary. They may not be furnished keys that allow access to the workroom areas. Other types of building keys may be furnished to nonpostal occupants, providing there is an official need.

242.3 Contractors

Keys may be furnished to contractors for exchange of mail in lobbies, vestibules, or lockers of post offices when those offices are not open. These keys must not permit access to workroom areas.

243Key Accountability

243.1 Inventory

Postmaster must keep an accurate inventory (including serial number and brand name of lock, total number of keys available, location of lock by door and/or room number, how and when disposed of) of all building keys and signed receipts for all assigned keys. Signed receipts should be obtained using a key log when keys are assigned.

243.2 Return of Keys

When an employee's duties no longer requires the use of an assigned key or the employee leaves the service, the key must be returned immediately. The date of return is then entered on the log. If keys used to operate exterior doors to the facility are not returned, the locks must be replaced or rekeyed.

243.3 Unassigned Keys

Store all unassigned keys in a secure place accessible only to the installation head or a designated alternate.

243.4 Key Survey

Conduct a semi-annual physical survey of all building keys. Pay particular attention to master keys, exterior entrance keys,and special keys such as those for registry cages, stamped enveloped rooms, employee record rooms, etc.

244Reporting Lost or Stolen Keys or Access Control Cards

244.1 Procedures

Immediately report a lost or stolen key or access control card to the installation head. Describe in detail the key or access control card, case, or key chain.

Section 3

ID BADGES

3ID Badges

31 Referenced Documents:

If there are other documents used as references list the here.

32 Purpose

Identification is issued for security control of access to postal premises and operations and to identify individuals as Postal Service employees. Every postal employee, postal contractor, and temporary employee, including casual employees, must have photo identification.

33 Scope

All personnel assigned an access control identification must wear it during official duty hours displayed on the outer garment over the left breast. When this is not possible the ID is worn in plain view on the belt or as prescribed by the installation head.

34Accountability Procedures

The responsible manager issues a photo identification card, to every postal employee and contractor.

341 All employees must wear and visibly display the identification card while officially employed and on duty.

342 All cards must include, at a minimum, the name of the employee, the facility to which they are assigned, an expiration date, and a photo of the employee.

343 While on duty away from the facilities servicing customers, each employee must wear and display their photo identification card.

35Access Control Badge and Postal Identification Card Custody/ Protection / Return

Protect identification or access badges by carefully controlling them. Keep supplies of unissued badges secure. Maintain a register that shows the employee's name and title, date of issuance, date of return, and the number, if any, of the identification badge issued. Access control identification badges controlled by a computer must automatically record usage. The computer must also be capable of off-loading the recorded accesses to a device for storage that allows retrieval at a later date. Mutilate and destroy access badges that cannot be reissued or are damaged.

All identification is accountable property and must be surrendered when leaving the Postal Service or when a contract is terminated. Employees who are issued identification must return such at the time of separation or transfer.

Take every precaution to prevent identification from falling into the hands of unauthorized persons. Employees must immediately report to their supervisors a lost or damaged identification. Report recovered identification promptly.
ions. (DM-901 723)

Section 4

CCTV Security System Maintenance& Repair Guidelines

4CCTV Security System Maintenance

41Referenced Documents:

If there are other documents used as references list the here.

42Purpose

This Security Guideline provides a national standard for the effective use and timely repairs of Closed Circuit Television (CCTV) security systems. These guidelines ensure appropriate attention to CCTV equipment issues.

43 Scope

The Postal Service uses CCTV systems for the protection of its employees, integrity of the mail, and postal assets. CCTV systems that are required and/or authorized are part of the overall security enhancement program and must be properly maintained in working condition at all times. The intent of this document is to set forth guidelines for the maintenance and/or repair of CCTV security systems.

44General Security Responsibility

441 Authorizations

Do not purchase closed circuit television (CCTV) systems, access-control systems, burglar or duress alarms, or fencing without first completing a risk assessment of the facility.

442 Policy

CCTV systems are for the protection of employees, mail, and postal assets, and to monitor automated mail flow operations. The purpose of CCTV systems is to provide visual verification in conjunction with intrusion detection devices or exit alarms and doors equipped with exit alarms or access control devices. CCTV systems are to function as deterrents, and if a crime occurs in the monitored area, to record evidence of it. The administrative and security uses of CCTV systems are limited to the following:

442.1 CCTV systems are installed to view parking lots, building exteriors, employee and visitor entrances, other access controlled entrances, emergency egress only, post office box areas, public access areas, and designated high-value locations, such as registry areas.

442.2 CCTV systems do not utilize “dummy” or nonfunctioning CCTV cameras.

443 Responsibility

The installation head and/or postal security unit will be responsible for CCTV systems.

45 Scheduled Maintenance

Routine and preventive maintenance is the responsibility of the installation head and/or the postal security unit.

CCTV System Maintenance/Operating Tips

A. The system should be set to operate and record in 24-hour mode, depending on the type of recorder in use in your office. The recorder must be recording continuously.

B. Check daily the system's time and date stamp for accuracy.

C. Check to ensure that none of the cameras are blocked by equipment or other obstructions.

Section 5

VEHICLE SECURITY

5 Vehicle Security

51 Referenced Documents:

52 Purpose

Provide the current policies and procedures for the Vehicle Security Program.

The postal fleet is a recognized and accepted presence throughout the cities and communities we serve. As an extension of the high public trust and confidence placed in our employees, postal vehicles have ready access to all manner of delivery points across the country.

Potential criminal use of postal vehicles to take advantage of the public trust or our delivery point access cannot be underestimated. Therefore, security of postal vehicles and vehicletags must be maintained at all times.

53 Scope

The Vehicle Security Program encompasses all facets of security involving vehicles, including license plates, vehicle decals/logos, vehicle administration and vehicle maintenance facility operations.

54 General Security Responsibility

541 Securing Vehicles

514.1 All postal managers with vehicles assigned to their locations must maintain proper vehicle security procedures.

541.2 Vehicles must be locked whenever the employee cannot maintain the vehicle in direct, full sight and fully ensure that neither the vehicle's interior nor its contents are tampered with.

541.3 Protect mail at all times. Keep the vehicle doors locked except when loading and unloading the vehicle. For vehicles with separate driver and cargo compartments, only working mail should be kept in the driver's compartment while performing delivery and collection duties.

541.4 Ensure that inoperable or malfunctioning vehicle locks are reported and repaired promptly. (HQ COO Memorandum, Vehicle Security, November 14, 2003)

542 License Plates

542.1 Vehicles and license plates must be physically inventoried and accounted for each week.

542.2 All license plates are to be installed by riveting or, as a minimum level of security, with tamper-resistant screws.

2.3. Tesis Tasarım Standartları

Sayfaya Geri Dön

Example Document for Facility Design Standards

(S58, 5.1.2)

Security Fencing

General

Security fencing (chain link) is required for every facility greater than 10,000 square feet. The fencing surrounds the private areas of the site compound. Access to the sides and rear of the building is provided as required through fence gates.

If local regulations or other entities oppose the use of fencing or walls, proposed alternatives should be approved in writing by the appropriate managers or security unit. Acceptable alternatives to fencing include natural barriers (e.g., earth berms, boulders, lakes, waterways, and bushes with thorns). Any alternative requests should be considered in conjunction with a risk assessment.

If a chain-link fence is not in keeping with neighborhood aesthetics or local zoning ordinances, then provide a 6-foot high, nonscalable wall or decorative fence. Thick interlocking bushes with thorns may be used; however, a low fence is required to keep pedestrians from walking into the bushes.

A deviation request must be submitted before approving alternatives.

Perimeter Fencing

Construction

Perimeter fencing, including gates, must be constructed of 9-gauge (minimum) steel wire with no more than 2-inch mesh fabric chain links.

Perimeter fencing and gates must be 6-feet high. In some cases an higher chain link fence with a top guard may be required as a result of the risk assessment. If local codes forbid or the community objects to perimeter fencing, then a written request to deviate is required.

If vandalism to the building or the vehicles occurs, then the local government and community are notified that a top guard will be installed. The design of the top guard must meet the following specifications:

a. Face outward and upward at a 45-degree angle.
b. Able to be mounted on top of the fence or wall to increase the height by 1 foot.
c. Be manufactured of three strands of 12 1/2-gauge, double-twisted barbed wire with four-point barbs closely spaced.

Fencing must be in straight lines and terminate at ground level on a paved surface or on firm nonshifting soil. Install a horizontal rail at the bottom of the fence and a tension wire at the top of the fabric.

Location

Provide perimeter fencing as follows:

a. Around the vehicle maneuvering and storage compound and around the employee parking lot if it is not economical to fence the entire site. (*Example*: If a site covers 10 acres and only 3 acres are being developed, typically only the immediate area requires fencing. The remaining land is to be posted around the perimeter every 100 feet with "No Trespassing" signs stating that the land is private property.)
b. Along street frontage enclose the paved parking and maneuvering areas for employee and Postal vehicles.
c. Along abutting buildings on both sides of public areas.

Clear Zone

The clear zone is defined as the area on either side of the fence that provides visibility adequate to discourage any criminal activity. The clear zone is located inside the fence and must be free of outbuildings, places of concealment, and points of unauthorized entry to the facility or Post vehicles and equipment.

If possible, the clear zone is to be 10 feet on either side of the fence. However, this is not always possible due to the location of the property line in relation to the fencing. Select vegetation to be planted in this zone based on growth potential. The clear zone must have only low shrubbery (2 to 3 feet maximum) if planting cannot be limited to grass. In addition, leave a distance of 2 feet between plantings and the exterior side of the fence, if possible.

Gates

Gates must be sized to permit safe and efficient access of passenger vehicles, trucks, semi-trailers, and emergency (fire) equipment. The gates must be lockable.

When the gates are closed, the continuous distance between the bottom of the gate and the paved surface must be no more than 4 inches high.

Gates do not need to be designed with both sides using the same type of operation. Gates can be a combination of slide gate and swing gate. No gate is to be longer than half the width of the road or driveway it serves, unless it is a sliding gate.

Employee Parking and Maneuvering Area Fencing

Employee parking and maneuvering area fencing is used to separate those areas at mail processing and delivery-unit-only facilities. Employee parking and maneuvering area fencing must be constructed of 6-foot-high chain-link fencing without a top guard. Other standards for perimeter fencing apply.

Security Lighting

General

Facilities must have basic security lighting to maintain acceptable levels of facility protection. This includes lighting at the following:

a. Entrance gates.
b. Employee entrances.
c. Vestibule entrances.
d. Areas around the building's perimeter and perimeter security fencing.
e. Areas not open to the general public.
f. Customer parking and entrances.

Exterior CCTV Security System

General

Buildings that meet the criteria for computerized access control systems under must have an exterior CCTV security system.

A full justification, which includes crime statistics and other environmental data, is to be provided in writing. The exterior security system encompasses exterior lighting as well as access control and CCTV. When the electronic system is installed, there must be sufficient lighting throughout the site so that the cameras can operate effectively and information is properly recorded.

Access Control System

A computerized card access control system is required for facilities meeting at least one of the following requirements:

a. Two hundred or more employees.
b. Revenue in excess of XX number of dollars.
c. Sixty-thousand or more square feet.
d. Other facilities that do not fall in any one of the above categories can be considered for a control system after a risk assessment has been completed.

Facilities not meeting the above specifications need to establish a robust physical access control program without the use of computerized systems. These facilities may use mechanical access control devices or electromechanical access control devices for establishing their physical access control programs. However, such a program does not necessarily mean that the physical access control program be computerized. The decision to install a computerized physical access control system for a facility not covered above should be based on a risk assessment.

Employee parking lots must have both a traffic arm and a manual gate at baseline security facilities and a motorized gate at high-risk locations. The vehicle access readers can be designed to work with an external device mounted on a car or with badges issued to the employees. Depending on other risks, equipment such as horizontal bars may be installed over the entry point to limit the size of vehicles entering the parking lot or gaining access to the building.

Turnstiles, auto-closing gates, or motorized gates are required for all pedestrian entrances. Turnstile-type gates are used in high-risk areas or where there is a problem with employee tailgating. Auto-closing and motorized gates are used in lower risk areas for accommodating the handicapped. At high-risk locations, additional entry security measures may be implemented.

Mail Processing Facilities or Areas

General Security Standards

The building entry must be clearly visible and, if possible, a single point of entry should accommodate both visitors and employees. The entryway must be designed to deny customers and other outsiders' access into the remainder of the facility and to keep off-duty employees and visitors from having access to the workroom after they enter the building.

Employee Entrance

Mail processing facilities must be designed with a single employee entrance. Site layout must provide safe access to the entrance (i.e., employees should not have to cross a major road or the access drive to the maneuvering area to reach the entrance). Situate the entry location so as to accommodate employees driving to work, being driven to work, or using public transportation. Site layout and parking lots must be adjusted to meet the standards outlined above.

Visitor and Administrative Entrance

Access to the facility for both visitors and administrative personnel must be through a single entrance; however, once visitors are inside, a separate doorway must prevent visitor access to administrative operations. The parking area for visitors must be separate from the employee parking area but in close proximity to the front entrance.

2.4. Anahtar Logları

Sayfaya Geri Dön

Key Accountability Log

Employee Name	Key Set No.	Issue Date	Issue Time	Signature	Return Date	Return Time	Supervisor Initials

2.5. Sürekli Güvenlik Önlemleri

Sayfaya Geri Dön

ALL EMPLOYEE
SECURITY AWARENESS BRIEFING

CHALLENGING/GREETING STRANGERS

The following approach may be used when challenging and/or greeting a stranger in your work area:

It is important to know how to approach a stranger who is not wearing a badge, someone who you do not see every day. You must keep in mind that it is your facility and it is your security that you are trying to protect. The first thing you do is introduce yourself and politely ask, “May I help you find someone?” You then have a few options, you can either call a supervisor to help the stranger, or call the office suggested by the stranger and have another employee come to your location and escort the person. In either case, you should wait for someone to help the individual and your job is done. One thing is certain: you absolutely should challenge unknown persons on the workroom floor. If the person resists, or tries to confront you, don’t pursue them. It’s time to call your supervisor, building security personnel or a postal police officer. It is not your job to get into a physical confrontation with a stranger. When you approach people remember that you are helping yourself and fellow employees. Remember that workplace security is good business and it’s personal.

2.6. Değerlendirme Gereci

Sayfaya Geri Dön

Standard	Sect.	Section Name	Sub-section	Requirement (standard language)	Onsite or Pre-	Question to:	Question	Response
S58	5.1.1	Risk assessment and facility security plans	5.1.1.1	An annual risk assessment must be conducted to identify each critical facility, such as the DO office of exchange. The assessment must take into consideration the postal assets and operations at the facility, the general crime rate of the area and other contributing factors that increase the likelihood of criminal incidents.	Both onsite and preassessment	DO security	Do you conduct an annual risk assessment for each critical facility (the office of exchange is one critical facility, but you may have more)? If so, would you please provide two recent risk assessment reports for our review?	
S58	5.1.1	Risk assessment and facility security plans	5.1.1.2	For each critical facility, a detailed written facility security plan must be developed and maintained. The facility security plan contains all of the following control measures: • general facility design standards; • perimeter barriers; • perimeter windows, doors or other openings; • lighting; • locking mechanisms and key controls.	Both onsite and preassessment	DO security	Do you have a written facility security plan for each critical facility? If yes, provide a copy of the facility security plan for each critical facility.	
S58	5.1.2	Critical facility design standards	5.1.2.2	A designated program of annual inspection and repair shall be conducted to assure the integrity of structures.	Both onsite and preassessment	DO security	Do you conduct a program of annual inspection and repair to assure the intgrity of facility structures? If so, please provide copies of the documented program plan and two most recent inspection reports.	
S58	5.1.2	Critical facility design standards	5.1.2.2	A designated program of annual inspection and repair shall be conducted to assure the integrity of structures.	Both onsite and preassessment	DO operations	Have you conducted repairs based on inspection report? If yes, please provide copies of the repair records for the last two inspection reports?	
S58	5.1.3	Perimeter barriers	5.1.3.2	Weekly inspections of the perimeter barriers shall be conducted to ensure their integrity.	Both onsite and preassessment	DO security	Do you conduct weekly inspections of the perimeter barriers? If yes, please provide the last two weekly inspection reports?	
S58	5.1.6	Locking mechanisms and key controls	5.1.6.2	Key controls A Key Control system shall be maintained for adequate key accountability. The Key Control system shall be administered by the Postal Security Unit or the respective postal facility manager. The system registers and records the issuance of keys and protects access to non-issued keys through the maintenance of a locked key storage location.	Both onsite and preassessment	DO security	Do you have a Key Control system? If so, please describe.	

Standard	Sect.	Section Name	Sub-section	Requirement (standard language)	Onsite or Pre-	Question to:	Question	Response
S58	5.1.6	Locking mechanisms and key controls	5.1.6.2	Key controls A Key Control system shall be maintained for adequate key accountability. The Key Control system shall be administered by the Postal Security Unit or the respective postal facility manager. The system registers and records the issuance of keys and protects access to non-issued keys through the maintenance of a locked key storage location.	Both onsite and preassessment	DO security	Is someone clearly designated as responsible for maintaining the Key Control system? Who?	
S58	5.1.6	Locking mechanisms and key controls	5.1.6.2	Key controls A Key Control system shall be maintained for adequate key accountability. The Key Control system shall be administered by the Postal Security Unit or the respective postal facility manager. The system registers and records the issuance of keys and protects access to non-issued keys through the maintenance of a locked key storage location.	Both onsite and preassessment	DO security	Does the Key Control system register and record the issuance of keys? If yes, provide the key issuance record or register (log).	
S58	5.1.6	Locking mechanisms and key controls	5.1.6.2	Key controls A Key Control system shall be maintained for adequate key accountability. The Key Control system shall be administered by the Postal Security Unit or the respective postal facility manager. The system registers and records the issuance of keys and protects access to non-issued keys through the maintenance of a locked key storage location.	Both onsite and preassessment	DO security	Are non-issued keys protected in a locked key storage location?	
S58	5.2.1	Access control measures: General	5.2.1.1	Levels of Access Control: Access control measures shall prevent unauthorized access to mail, and mail conveyance vehicles, in critical facilities. The appropriate level of access control shall be implemented at every critical facility to protect and secure postal assets. NOTE Access control may be a manual process utilizing fixed security guard posts at entry/egress points to verify the identity of the individual or vehicle entering the secure area. Access control measures may also consist of simple or complex electronic systems to verify and permit access to the secure areas. Regardless of the technological aspects of the methods utilized, the system possess the ability to adequately screen and differentiate the access privileges of emloyees, visitors, service providers, and vendors at all points of entry. The access control system in a critical facility is segmented to ensure that employees, visitors, service providers and vendors be only permitted access to those areas of a facility where they have work functions or conduct business.	Both onsite and preassessment	DO security	How do the access control measures implemented prevent unauthorized access to mail, and mail conveyance vehicles in critical facilities?	

Standard	Sect.	Section Name	Sub-section	Requirement (standard language)	Onsite or Pre-	Question to:	Question	Response
S58	5.2.1	Access control measures: General	5.2.1.1	Levels of Access Control: Access control measures shall prevent unauthorized access to mail, and mail conveyance vehicles, in critical facilities. The appropriate level of access control shall be implemented at every critical facility to protect and secure postal assets. NOTE Access control may be a manual process utilizing fixed security guard posts at entry/egress points to verify the identity of the individual or vehicle entering the secure area. Access control measures may also consist of simple or complex electronic systems to verify and permit access to the secure areas. Regardless of the technological aspects of the methods utilized, the system possess the ability to adequately screen and differentiate the access privileges of emloyees, visitors, service providers, and vendors at all points of entry. The access control system in a critical facility is segmented to ensure that employees, visitors, service providers and vendors be only permitted access to those areas of a facility where they have work functions or conduct business.	Both onsite and preassessment	DO security	Is the appropriate level of access control implemented at every critical facility to protect and secure postal assests? What type of access control is used?	
A	5.2.1	Access control measures: General	5.2.1.1	Levels of Access Control: Access control measures shall prevent unauthorized access to mail, and mail conveyance vehicles, in critical facilities. The appropriate level of access control shall be implemented at every critical facility to protect and secure postal assets. NOTE Access control may be a manual process utilizing fixed security guard posts at entry/egress points to verify the identity of the individual or vehicle entering the secure area. Access control measures may also consist of simple or complex electronic systems to verify and permit access to the secure areas. Regardless of the technological aspects of the methods utilized, the system possess the ability to adequately screen and differentiate the access privileges of emloyees, visitors, service providers, and vendors at all points of entry. The access control system in a critical facility is segmented to ensure that employees, visitors, service providers and vendors be only permitted access to those areas of a facility where they have work functions or conduct business.	Both onsite and preassessment	DO security	Is the access control system in a critical facility segmented to ensure that employees, visitors, service providers, and vendors are only permitted access to those areas of a facility where they conduct business or a work related need for entry?	

Standard	Sect.	Section Name	Sub-section	Requirement (standard language)	Onsite or Pre-	Question to:	Question	Response
S58	5.2.2	Access control systems for employees, visitors, service providers and vendors	5.2.2.1	System may be manual or automated. Different sections of the standard apply depending on the type of system. Characterize this practice based on whether one type or the other is implemented. Use the remaining sections to characterize the conformance of the system based its type.	Preassessment	DO security	Is the access control process for the secure (non-customer) areas of all postal facilities automated or manual?	
S58	5.2.2	Access control systems for employees, visitors, service providers and vendors	5.2.2.2	Manual access control: Prevent unauthorized entry a. Manual access control system ii. uniformed Security Guards, a receptionist or other personnel staff shall be at entry/egress points to verify the entry privileges for each individual; Note 1 The carriage of personal belongings, e.g. bags, and the limitation thereof as well as the institution of search procedures should be considered.	Both onsite and preassessment	DO security	IF SYSTEM IS MANUAL: How are entry and egress points protected to prevent unauthorized entry? How are the entry privileges verified for each person entering?	
S58	5.2.2	Access control systems for employees, visitors, service providers and vendors	5.2.2.3	Manual access control: Documentation and training ii. the manual process shall be documented in a standard operating procedure; iii. training and instructions shall be provided to the respective personnel administering the program and the individuals stationed at the fixed access control point;	Both onsite and preassessment	DO security	IF SYSTEM IS MANUAL: Do you have a manual access control system or process documented and in place for critical postal facilties? If yes, provide documentation.	
S58	5.2.2	Access control systems for employees, visitors, service providers and vendors	5.2.2.3	Manual access control: Documentation and training ii. the manual process shall be documented in a standard operating procedure; iii. training and instructions shall be provided to the respective personnel administering the program and the individuals stationed at the fixed access control point;	Both onsite and preassessment	DO security	IF SYSTEM IS MANUAL: Are training and instructions provided to the respective personnel administering the program and the individuals stationed at the fixed access control point?	
S58	5.2.2	Access control systems for employees, visitors, service providers and vendors	5.2.2.4	Manual access control: Visitors and vendors iv. a registration system shall be maintained to record entries of non-employees into secure areas of the critical facility.	Both onsite and preassessment	DO security	IF SYSTEM IS MANUAL: Are visitors to the facility escorted at all times? Are service providers and vendors escorted? Under what circumstances are vendors and service providers not escorted? (Are unescorted service providers and vendors pre-cleared and/or badged?)	

Standard	Sect.	Section Name	Sub-section	Requirement (standard language)	Onsite or Pre-	Question to:	Question	Response
S58	5.2.2	Access control systems for employees, visitors, service providers and vendors	5.2.2.5	Automated access control: Prevent unauthorized entry b. An automated (electronic) access control system The system shall be designed to prohibit unauthorized entries of individuals through the entry/egress points and only through a single access system or process and shall be a single access system to only permit entry for the respective badge holder which activated the access point. Note 2 A single access system can also be accomplished by assigning a uniformed security guard or other personnel to a fixed post to monitor the entries/egress from the access point. If the entry/egress point is not monitored, physical access control equipment (turnstiles, access gates and doors) activated by badge readers or electronic keys should be used.	Both onsite and preassessment	DO security	IF SYSTEM IS AUTOMATED: How are entry and egress points protected to prevent unauthorized entry? Are guards or other personnel posted or is a turnstile or other mechanical means used? Is the system designed so that only a single entry is allowed for the badge holder who activated the system (in other words, how does the system prevent tail-gating)?	
S58	5.2.2	Access control systems for employees, visitors, service providers and	5.2.2.6	Automated access control: Visitors and vendors A visitor registration system shall be implemented to record entries of non-employees into secure areas of the critical facility.	Both onsite and preassessment	DO security	IF SYSTEM IS AUTOMATED: Is a visitor registration system maintained to record entries of non-employees into the secure areas of the critical facility?	
S58	5.2.2	Access control systems for employees, visitors, service providers and vendors	5.2.2.6	Automated access control: Visitors and vendors A visitor registration system shall be implemented to record entries of non-employees into secure areas of the critical facility.	Both onsite and preassessment	DO security	IF SYSTEM IS AUTOMATED: Are visitors to the facility escorted at all times? Are service providers and vendors escorted? Under what circumstances are vendors and service providers not escorted? (Are unescorted service providers and vendors pre-cleared and/or badged?) Are visitors issued electronic access devices? (NOTE: standard requires that visitors NOT be issued such devices)	
S58	5.2.3	Access control systems for vehicles	5.2.3.3	A manual or automated access control system shall be used to ensure unauthorized vehicles do not gain access into the secure exterior operations area.	Preassessment	DO security	Is a manual or automated system used to control access to ensure that unauthorized vehicles do not gain access into the secure exterior operations area? If a manual system is used, please be prepared to share documentation on the system.	

Standard	Sect.	Section Name	Sub-section	Requirement (standard language)	Onsite or Pre-	Question to:	Question	Response
S58	5.2.3	Access control systems for vehicles	5.2.3.3	A manual or automated access control system shall be used to ensure unauthorized vehicles do not gain access into the secure exterior operations area.	Preassessment	DO security	How is access controlled to ensure unauthorized vehicles do not gain access into the secure exterior operations area? If a manual system is used, request to see documentation on the manual system. If an automated system is used, request a demonstration.	
S58	5.2.4	Identification systems	5.2.4.3	The Postal Security Unit or other postal managers shall be responsible for the control, issuance and removal of employee, visitor and contractor identification badges. A process shall be maintained to report and communicate employee information.	Both onsite and preassessment	DO security	What is the process for the control, issuance and removal of employee, visitor and contractor identification badges? Who is responsible for that process?	
S58	6,1	Personnel Security and Training General	6.1.1	General Important to postal operations are its personnel and as such it is fundamental to operators that any potential security risks that are posed as a result of new employees or parties providing services entering into the business, as well as those resulting from the redeployment of employees onto roles with different vetting or training requirements are minimized. Personnel security and training shall be deployed in order to reduce and minimize security risks to the business, its customers and employees.	Both onsite and preassessment	DO security	This question may also be asked of DO Human Resources. Is training conducted for new and re-assigned personnel in an effort to minimize security risks to the business, its customers and employees? What is the frequency and type of training conducted?	
S58	6,2	Personnel security and hiring processes	6.2.1	Background checks (criminal history or police checks) for all career employees shall be conducted consistent with national legislation.	Both onsite and preassessment	DO security	This question may also be asked of DO Human Resources. Are background checks performed for all career employees consistent with national legislation? How often are they repeated or updated?	
S58	6,2	Personnel security and hiring processes	6.2.1	Employee hiring The personnel selection and hiring policy shall be documented for all employees working within the facilities of the DO or handling mail at external locations.	Both onsite and preassessment	DO human resources	Do you have a documented personnel selection and hiring policy for employees working within the facilities of the DO or handling mail at external locations? If yes, please provide a copy of the hiring policy for review.	
S58	6,2	Personnel security and hiring processes	6.2.1	The hiring policy shall be consistent with national legislation to ensure prospective and current employees and contractors are qualified to perform postal duties as a person of integrity.	Both onsite and preassessment	DO human resources	Is your selection and hiring policy for employees consistent with national legislation to ensure that people performing postal duties are suitable for the function?	

Standard	Sect.	Section Name	Sub-section	Requirement (standard language)	Onsite or Pre-	Question to:	Question	Response
S58	6,2	Personnel security and hiring processes	6.2.1	The hiring process includes interviews, pre-employment data verification and other screening measures commensurate with positions or duties.	Both onsite and preassessment	DO human resources	How are candidate employees evaluated before hiring? Interviews? Verification of pre-employment data? Other checks measures?	
S58	6,2	Personnel security and hiring processes	6.2.2	The termination process shall be documented for employees and contractors.	Preassessment	DO human resources	Do you have a documented termination process? If yes, please be prepared to share the documentation.	
S58	6,2	Personnel security and hiring processes	6.2.2	The termination process shall ensure the timely return of identification documents, access control devices, keys, uniforms and other sensitive information.	Both onsite and preassessment	DO human resources	Does the termination process ensure the timely return of identification documents, access control devices, keys, uniforms and other sensitive information?	
S58	6,2	Personnel security and hiring processes	6.2.2	A record system shall be maintained to prevent re-hiring of employees or contractors who have been terminated due to misconduct	Both onsite and preassessment	DO human resources	Do you have a record system to prevent rehiring employees or contractors who have been terminated for cause?	
S58	6,2	Personnel security and hiring processes	6.2.3	A process shall be maintained to report and communicate employee performance and misconduct.	Both onsite and preassessment	DO human resources	This question may also be asked of DO Security. What is the process for reporting and communicating employee performance and misconduct?	
S58	6,3	Contractor security requirements	6.3.1	Contractor compliance Contractors used to perform mail handling/transport operations or other sensitive functions shall apply personnel security measures equivalent to the DO as described in section 6.2.	Preassessment	DO operations	Are contractors used to perform mail handling/transport operations or other sensitive functions for the DO? NOTE: If the answer to this question is yes, then section 6.2 applies. If no, the remaining questions for 6.2 should be skipped.	
S58	6,3	Contractor security requirements	6.3.2	Contractor Security The contractor should inform the DO of any personnel findings or decisions which could pose a potential security risk to the operation.	Both onsite and preassessment	DO operations	Question applies if contractors are used. Does contractor inform the DO of any personnel findings or decisions which could pose a potential security risk to the operation?	
S58	6,4	Awareness and training measures	6.4.1	A security awareness training program shall be documented and maintained for all employees and contractors.	Both onsite and preassessment	DO security	Do you have a security awareness program? Is it documented and maintained for all employees and contractors? If yes, please be prepared to share the documentation for review.	

Standard	Sect.	Section Name	Sub-section	Requirement (standard language)	Onsite or Pre-	Question to:	Question	Response
S58	7,1	Transportation and conveyance security requirements for DO's and postal contractors	7.1.1	Documented mail conveyance security procedures The DO and authorized contractors shall document processes and procedures for security of the mail by all modes (air, road, sea and rail) of transportation. The DO shall comply with all applicable national legislation regarding transportation standards.	Both onsite and preassessment	DO security	Do you have a documented process for security of the mail by all modes (air, road, sea and rail) of transportation? Does it also apply to contractors? If yes, please be prepared to provide the documentation for review. Does the DO comply with all applicable national legislation regarding transportation standards?	
S58	7,1	Transportation and conveyance security requirements for DO's and postal contractors	7.1.2	Restricted access to mail Access to mail shall be restricted as appropriate to postal employees or contractors with mail handling responsibilities.	Both onsite and preassessment	DO security	How is access to mail restricted to postal employees or contractors with mail handling responsibilities?	
S58	7,1	Transportation and conveyance security requirements for DO's and postal contractors	7.1.5	Mail transport vehicle key accountability Vehicle cabin and ignition keys for all transport vehicles shall be secured from unauthorized access. A key accountability process shall be maintained.	Both onsite and preassessment	DO security	How are vehicle cabin and ignition keys for all transport vehicles secured from unauthorized access? Do you have a key accountability process in place? If so, how is that accountability process maintained; who is responsible for it?	
S58	7,1	Transportation and conveyance security requirements for DO's and postal contractors	7.1.6	Risk assessment of routes Routes, schedules and planned stops shall be assessed for risk and, if necessary, an additional security measure shall be initiated to mitigate the risk.	Both onsite and preassessment	DO security	Are routes, schedules and planned stops assessed for risk? If yes, what additional security measures are used to mitigate risk?	
S58	8,1	Compliance audit program and oversight	8.1.1	Annual compliance audits An annual compliance audit shall be conducted by personnel independent of the critical facility management team.	Both onsite and preassessment	DO security	Is an annual compliance audit conducted on the mail security program by personnel independent of the management team? Who conducts the audit? Please be prepared to provide the most recent report.	
S58	8,1	Compliance audit program and oversight	8.1.2	Compliance audit personnel The individuals conducting the compliance audit review shall be afforded the necessary authority to obtain relevant information and to enforce corrective action.	Both onsite and preassessment	DO security	How are the individuals conducting the compliance audit review afforded the necessary authority to obtain relevant information and to enforce corrective action?	

Standard	Sect.	Section Name	Sub-section	Requirement (standard language)	Onsite or Pre-	Question to:	Question	Response
S58	8,1	Compliance audit program and oversight	8.1.3	Compliance audit content The compliance audit review program covers the entire mail security program to ensure implementation of security requirements. The compliance audit review program shall include but not be limited to an emphasized focus on: − facility security; − personnel security; − transportation and conveyance security.	Both onsite and preassessment	DO security	Does the compliance audit review program cover the entire mail security program to ensure implementation of security requirements? Do the audits address facility security, personnel security, transportation and conveyance security?	
S58	8,1	Compliance audit program and oversight	8.1.4	Compliance audit objectivity The DO shall ensure that the management of the compliance audit review program shall be independent from individuals responsible for the implementation of the security requirements.	Both onsite and preassessment	DO security	How do you ensure that the compliance audit review program remains independent from those responsible for the implementation of the security requirements?	
S58	8,1	Compliance audit program and oversight	8.1.5	Compliance audit results Records of the compliance audits and recommendations shall be maintained. The result of the compliance audits shall be reported to the executive management of the DO. Follow up actions are to be monitored and documented.	Both onsite and preassessment	DO security	How are results of the compliance audits reported to the executive management of the DO?	
S58	9,1	Postal Security Unit for Prevention and Investigative Management	9.1.1	Documented postal security program The DO has a documented security program covering the areas of prevention and investigation for the protection of mail, employees, partners, customers and postal assets. This shall be communicated to all employees. EXAMPLE: Equipment, vehicles, uniforms, information technology, etc.	Both onsite and preassessment	DO security	Does the DO have a documented security program covering the areas of prevention and investigation for the protection of mail, employees, partners, customers and postal assets? If so, please be prepared to share the documentation for review.	
S58	9,1	Postal Security Unit for Prevention and Investigative Management	9.1.2	Postal security unit personnel The DO shall have a dedicated Postal Security Unit or dedicated personnel to perform safety and security measures. The staff members dedicated to these functions shall be commensurate with the size and operations of the DO.	Both onsite and preassessment	DO security	Does the DO have a dedicated Postal Security Unit or dedicated personnel to perform safety and security measures? How many staff members are included in the unit or are responsible for performing safety and security? Do you have enough personnel dedicated to security functions? If not, what is not being done as a result of not having enough staff?	

Standard	Sect.	Section Name	Sub-section	Requirement (standard language)	Onsite or Pre-	Question to:	Question	Response
S58	9,1	Postal Security Unit for Prevention and Investigative Management	9.1.3	The dedicated Postal Security Unit or dedicated security personnel shall perform periodic facility and process security reviews.	Both onsite and preassessment	DO security	Does the dedicated Postal Security Unit or dedicated security personnel perform periodic facility and process security reviews? Please be prepared to provide documentation of these reviews.	
S58	9,2	Disaster recovery, emergency preparedness, and business continuity planning	9.2.1	Documented crisis plan The DO shall document and communicate to the appropriate employees a crisis plan to ensure the security of mail, employees, customers and postal assets in the event of a man-made or natural disaster that would affect the flow of mail or postal operations.	Both onsite and preassessment	DO security	Does the DO document and communicate to the appropriate employees a crisis plan to ensure the security of mail, employees, customers and postal assets in the event of a man-made or natural disaster that would affect the flow of mail or postal operations. If yes, please be prepared to provide a copy of the plan.	
S58	9,2	Disaster recovery, emergency preparedness, and business continuity planning	9.2.2	Documented business continuity plan The DO shall have document and communicate to the appropriate employees a business continuity plan to minimize postal interruption in the event of significant incident which might impact domestic or international postal operations.	Both onsite and preassessment	DO security	Does the DO document and communicate to the appropriate employees a business continuity plan to minimize postal interruption in the event of significant incident which might impact domestic or international postal operations? If yes, please be prepared to provide a copy of the plan.	
S59	5,1	Custody of international airmail	5.1.1	Control custody of international airmail The DO shall maintain direct custody (by DO or designee) and control of international mail intended for carriage by air from the time of acceptance until dispatched to the carrier/agent/designee. When a DO arranges to have a contractor or other entity accept international airmail on its behalf, the DO remains responsible for acceptance and handling of the mail. As such, the DO should have processes in place whereby the contractor or other entity shall comply with these standards.	Both onsite and preassessment	DPO security	Please describe the custody procedures for international mail intended for carriage by air. Are these procedures also followed by contractors?	

Standard	Sect.	Section Name	Sub-section	Requirement (standard language)	Onsite or Pre-	Question to:	Question	Response
S59	5,2	Items exempt from screening	5.2.1	Define exempted items When dispatching mail consisting of international post items up to 500 grames, the DO may dispatch without additional screening if the DO has adhered to the security measures outlined in UPU S58. Note: There may be other applicable international and/or national regulations which may define different thresholds for exemptions. Any exemptions applied should be in agreement with the appropriate national legislation or regulation. UPU member countries may agree to permit exemptions from screening or the use of alternative security measures because of the special nature of some types of mail. Such exemptions should be clearly defined in UPU member Countries National Civil Aviation Security Program (NCASP).	Both onsite and preassessment	DPO security	IF mail pieces are exempted from screening have they been agreed upon with national authorities? **Due to security considerations and confidentiality it may not be appropriate to list exempted items in this report.** How are the items that are exempted from screening kept separate from items that are subject to screening?	
S59	5,3	Items to be Screened	5.3.2	Screen mail items The DO or designee shall screen items by at least one of the following methods in accordance with the requirements of their national aviation security program. As a minimum, the NCASP should reflect the standards and recommended practices set forth in ICAO Annex 17 and the guidance material in ICAO Aviation Security Manual, Doc 8973. –EDD; – EDS; – ETVD; – Manual Search; – Metal detection; – X-Ray equipments or other wave based systems.	Both onsite and preassessment	DPO security	Which mail screening standards are used? ICAO Annex 17 and the ICAO Aviation Security Manual, DOC 8973? **Due to security considerations and confidentiality it may not be appropriate to list screening standards in this report.**	
S59	5,4	High Risk Items	5.4.1	Define high risk mail items Mail that requires additional security measures beyond baseline procedures is considered high risk. Mail or mail items can be considered high risk if there are: – anomalies in its nature that give rise to suspicion such as evidence of tampering; – due to its nature, baseline security measures alone are unlikely to detect prohibited articles as defined in the UPU postal security standards; – specific intelligence or threat information about it; – reasons to suspect that it contains or poses a threat based on risk assessment by an appropriate authority for aviation security, aircraft operators or other actors in the supply chain.	Both onsite and preassessment	DPO security	What is your definition for a high-risk mail item? Is that definition documented? Please be prepared to provide this documentation.	

Standard	Sect.	Section Name	Sub-section	Requirement (standard language)	Onsite or Pre-	Question to:	Question	Response
S59	5,4	High Risk Items	5.4.2	Screen high risk mail items The DO or designee shall screen high risk items by viewing the item or receptacle from two angles and complying with National legislation OR – utilizing a combination of two or more screening methods below: – manual search ; – X-Ray equipment; – EDD; – ETD.	Both onsite and preassessment	DPO security	Which screening methods are used to screen high risk mail items (pieces or receptacles)? **Due to security considerations and confidentiality it may not be appropriate to list screening methods in this report.**	
S59	5,5	Screening procedures for mail receptacles/bags	5.5.1	Screen mail receptacles/bags When authorized by their respective national authorities, the DO or designee shall utilize the technologies below to screen items already contained in receptacles/bags: – X-Ray screening technology that is the most appropriate for the particular item or receptacle: i. the DO shall X-ray one receptacle at a time to search for indications of unauthorized explosives, incendiaries, and other destructive substances or items. ii. mail receptacles containing commodities that are too dense to render an accurate X-ray image must be screened twice in succession, rotating the receptacle 90 degrees horizontally in either direction prior to screening it the second time, iii. if the X-ray image is unclear, shielded, or opaque or contains any unidentifiable anomalies, the DO must clear the X-ray image by removing each mail piece from the receptacle and re-screen the individual pieces. and/or – EDD; and/or – EDS.	Both onsite and preassessment	DPO security	Describe your screening process in detail for items already contained in mail receptacles or bags. Which technologies are being used? **Due to security considerations and confidentiality it may not be appropriate to list which technologies are being used in this report.**	
S59	5,6	Alarm resolution of suspicious items	5.6.1	Clear suspicious items If the DO or screening designee identifies an item which cannot be cleared (alarm) during the initial screening, the item shall not be handed over to a carrier until the item is determined to be "Safe to Fly": The item should be handled as a high risk item in accordance with Section 5.4 of these standards.	Both onsite and preassessment	DPO security	Please describe what happens when an item fails the initial screening. • What procedures do you follow to determine whether an item that fails initial screening is safe to fly? (Compare responses to standard)	

Standard	Sect.	Section Name	Sub-section	Requirement (standard language)	Onsite or Pre-	Question to:	Question	Response
S59	5,7	Notification Procedures	5.7.1	Isolation of failed mail pieces Cognizant of NCASP requirements, if the DO or screening designee cannot clear an item after following the procedures outlined above the mail item shall not be handed over, loaded or transported to any carrier/aircraft. The item shall be isolated in a secure location, controlled, and physically guarded to prevent unauthorized access.	Both onsite and preassessment	DPO security	When a suspicious mail item or receptacle cannot be resolved, what procedures are followed? What are the isolation and handling procedures for the suspicious mail item or receptacle?	
S59	5,7	Notification Procedures	5.7.2	Notification for failed mail pieces The DO or screening designee shall: – immediately contact the Ground Security Coordinator (GSC), host government authorities, Police, Fire Department, and/or Bomb Squad, according to local requirements; – inform entities identified of any additional international mail on the premises that was tendered or transferred with the suspect mail item.	Both onsite and preassessment	DPO security	When a suspicious mail item or receptacle cannot be resolved, what procedures are followed? What are the notification procedures? Do you notify - the Ground Security Coordinator (GSC)? - host government authorities, - Police, - Fire Department, and/or - Bomb Squad? Do you inform entities of any additional international mail on the premises that was tendered or transferred with the suspect mail item?	
S59	6,1	Measures for mail accepted/inducted for carriage on commercial aircraft	6.1.1	Mail security procedures The DO shall tender items to carriers, ground handling agents or other contractors for transport on aircraft in identifiable bags (receptacles) or containers affixed with the appropriate UPU forms or receptacle labels. After screening or the application of other security controls, mail shall be accounted for and protected from unauthorised interference prior to loading on an aircraft or secure exchange with the carrier, ground handling agent or other contractor. In accordance with their NCASP a DO who has applied screening and security controls may be required to provide a consignment security declaration to the aircraft operator. The NCASP may also require additional record keeping for the purposes of an audit trail that the DO may need to address.	Both onsite and preassessment	DO operations	After security controls have been applied, how is mail accounted for and protected from unauthorized interference prior to loading on an aircraft or secure exchange with the carrier?	

2.7. UPU Kriz Planlaması

Sayfaya Geri Dön

Crisis Management and Business Continuity Plan
Universal Postal Union

I. Executive Summary and Introduction

1.0 The combined Crisis Management and Business Continuity Plan sets out the policy and decision-making process for managing a physical crisis at the Universal Postal Union (UPU) International Bureau in order to maintain the mission critical functions of the Organization. It provides a management strategy for a coordinated response by the various offices and departments at the International Bureau. It identifies key players both at the policy and operational levels and explains their roles in the overall management of and response to crisis situations. It establishes the ground rules for activation of the Plan.

2.0 The combined Crisis Management and Business Continuity Plan cover the International Bureau in Berne, Switzerland.

3.0 The Crisis Management and Business Continuity Plan is structured in two parts. The first part, the Crisis Management Plan sets out the organizational elements of the crisis management structure, the roles of the different elements and the procedures for action. Specific arrangements have been made to use off-site premises to enable the mission critical functions to continue during and after a crisis.

4.0 The second part, the Business Continuity Plan provides for implementing the procedures in place so that core staff can perform the Critical Business Process of the UPU. The activation of this plan is closely linked to the Crisis Management Plan. However, the Business Continuity Plan will not be activated until the initial crisis is evaluated by the core staff and an assessment is made on how best to proceed with performing critical business processes.

5.0 During a crisis, it is imperative that the International Bureau transform itself into a centralized, single focus organization. This is to be accomplished by shortening lines of communication and centralizing communication flow, which in turn supports rapid and precise decision-making.

6.0 A critical element in the decision-making process is face-to-face interaction between senior managers in a secure location. This ensures that key managers are able to conduct a preliminary assessment of the nature and gravity of the crisis and take mitigation decisions promptly.

7.0 The combined plan will be subject to periodic review and revision to ensure that it remains accurate and timely. It includes elements which reflect all three major phases of an emergency or crisis – preventative actions which can be taken before a crisis occurs, responses appropriate to the nature of a crisis, and longer term recovery after a crisis, in the context of an overall business continuity plan. It does not include provisions for security and crisis management in the field, which belong more appropriately in the purview of UN Department of Safety and Security (UNDSS); however, it has drawn on the experience of UNDSS with emergencies in field situations.

8.0 In the preparation of the combined plan, advice has been sought from external experts in the field of emergency preparedness, and due account has been taken of the considerable body of planning and operational work in place within the United Nations common system of organizations and United Nations Headquarters.

Crisis Management and Business Continuity Plan
Universal Postal Union

Organizational chart of the International Bureau

Crisis Management and Business Continuity Plan
Universal Postal Union

II. Crisis Management Structure – Organizational elements, roles and procedures

1.0 The mission critical functions of the UPU are those core activities for which it is essential to ensure a level of continuity in the face of an emergency or crisis. They are functions in which the absence impairs and/or diminishes the capacity of the Organization to carry out its key mandates, places lives at risk and threatens physical assets, disrupts the political process and puts the role of the Director General at risk.

2.0 The broad elements that constitute the mission critical functions of the Organization at the International Bureau are:

2.1 The protection of the staff and assets of the Organization.

2.2 The ability of the Director-General to represent the Organization, to respond to the needs of the international postal community, to provide the means for diplomatic discourse and negotiation and to play a leadership role.

2.3 The provision of basic support services to enable the Director-General and his close advisors and Member Administrations to communicate, conduct business and implement decisions, even in a restricted or modified format or in a different location.

3.0 More particularly, the mission critical functions include:

3.1 The security and safety of the staff and assets.

3.2 The ability of the principal organs to conduct crucial meetings.

3.3 The ability to maintain information and communications technology services.

3.4 The maintenance of direction and oversight of critical operations.

3.5 Ensuring continuity of key financial operations.

3.6 Communications with the staff.

III. Crisis Management – Critical functions of the Director General

1.0 The continuity of the Director General's political functions and the exercise of his international leadership role are the paramount challenges for the Director General in a major crisis. The ability of the Director General to respond fully to the needs of the international postal community, to provide the mechanisms for diplomatic negotiation and action and to provide for his leadership, stand as the most critical functions of the office and communication with staff.

IV. Crisis Management – Critical personnel

1.0 Two entities directly manage a crisis situation. The *Senior Emergency Management Group (SEMG)* is responsible for the immediate policy decisions required to deal with the particular impact of the crisis. Decisions such as the continuation of scheduled

meetings/conferences, the suspension of routine operations, extraordinary procurement mandates, relocation or evacuation of staff and offices, and formal requests to the host country authorities for assistance, are examples that may need to be addressed.

1.1 The members of the SEMG are:

- Director General (Chairperson)
- Deputy Director General
- Director of DCC
- Director Operations and Technology
- Director of Legal Affairs and Ethics Bureau
- Director Finance
- Director Logistics
- Director Human Resources
- Head PTC
- Head of Cabinet

2.0 The Director General will serve as the chair of the SEMG. The DG will provide policy direction to the members of the COG.

3.0 The specific array of functions, most particularly internal and external communications, carried out by the Director of the DCC are determined not only by the circumstances and seriousness of the emergency itself, but by a range of other priorities dictated by international events.

4.0 For each member of the SEMG, an alternate has been designated, in the event that SEMG members become casualties in a major emergency incident, or are otherwise unavailable. The SEMG mirrors the crisis management structure at the United Nations Headquarters and the United Nations Office at Geneva.

5.0 The second entity is the *Crisis Operations Group (COG)*, comprising personnel from key administrative and support functions at the International Bureau. They serve as staff to the Director of Logistics, who is responsible for operational decisions and their implementation in accordance with the policy directives of the SEMG. In the event that the Director of Logistics is unavailable, the General Services and Conferences Program Manager will act as chairperson of the COG.

5.1 The members of the COG include:

- Human Resources Expert
- Program and Budget Expert
- Director of Legal Affairs and Ethics Bureau
- Communications Program Manager
- General Services and Conferences Program Manager
- Internal IT Program Manager
- Postal Security Expert

6.0 The following are the main tasks of each of the members of the COG:

6.1 The *Communications Program Manager* is responsible for keeping staff informed and for providing information and data on staffing, guidance to the COG Chairperson on communications with the staff, and briefing/counseling services to the staff of the

International Bureau.

6.2 Medical services will be coordinated through the *Human Resources Expert* with appropriate liaison with Swiss authorities including providing trauma support services to staff.

6.3 The *Program and Budget Expert* is responsible for maintaining essential financial transactions and for maintaining key financial management functions. This COG member provides guidance to the COG Chairperson on financial matters.

6.4 The *Director of Legal Affairs and Ethics Bureau* is responsible for providing legal advice and counsel to the Chairpersons of the SEMG and COG and will have contact with the Swiss Authorities on matters of Privileges and Immunities.

6.5 The *Communications Program Manager* will continue to carry out public information activities, to ensure the speediest recording and wide dissemination of statements and briefings or other activities by the Director General or other senior officials. This member will also establish press facilities and a briefing area for media at the location to which operations have been relocated, if necessary.

6.6 The *General Services and Conferences Program Manager* is responsible for the provision of essential services to support meetings, on an as-available basis in an emergency. This member is also responsible for the proper functioning of physical infrastructure systems and facilities throughout the International Bureau and makes recommendations on the viability of returning to normal operational conditions. The General Services and Conferences Program Manager arranges for the urgent procurement of goods and services related to mission critical functions.

6.7 The *Internal IT Program Manager* is responsible for servicing computer and telecommunications functions on a 24 hour basis, including the maintenance of leased lines and satellite communications.

6.8 The *Postal Security Expert* is responsible for immediate life/safety issues and for security related matters. This member maintains the Emergency Operations Centre and the Crisis Event Log and advises the SEMG on the current situation.

7.0 For each member of the COG, alternates have been designated, in the event that COG members become casualties in a major emergency incident, or are otherwise unavailable. The COG shall actively interact with the SEMG and the UNDSS at United Nations Headquarters. Chain of command and outside contact lists are maintained by the SEMG/COG on a confidential basis. All members and alternates of SEMG and COG should carry contact cards which list the relevant telephone, fax and email information for all members.

V. Crisis Management and Business Continuity– Alternate locations

1.0 Depending on the nature and severity of the crisis, arrangements are in place for alternative meeting points for the SEMG and the COG. Whenever feasible, they will be co-located or in close proximity to each other. The SEMG will decide on the specific location(s) to be used by the two groups and on the location of the Emergency Operations Centre.

2.0 In the event that the International Bureau premises are usable, the SEMG and COG will meet at the Emergency Operations Centre specified in Annex 1

3.0 If the International Bureau premises can no longer be used, the SEMG and COG would meet at the Alternate Emergency Operations Centre specified in Annex 1 (***currently, alternate locations are still being evaluated***)

4.0 In the contingency that the metropolitan Berne area becomes unsafe to continue operations, the United Nations Office at Geneva will be consulted to arrange alternate locations for the groups to relocate. Any new location will be reviewed and approved by the Swiss Permanent Mission.

5.0 The work of the COG is supported by a logistics team under the authority of the Director of Logistics. The team ensures that the above locations are available for use; ensures that the Crisis Management Plan is current and arranges periodic reviews and simulation exercises. The logistics team briefs the Director General and Deputy Director General on any events or developments which may require the activation of the Crisis Management Plan. This team updates data on SEMG and COG membership and alternates, vendors/external contacts, host country contacts and other entities that may be called on for assistance in a crisis.

VI. Hazard Analysis Matrix and Threat scenarios – severity of impact

1.0 Different threats or crises have different consequences in terms of their impact on the International Bureau, on its ability to discharge critical functions, and on the most appropriate type of response to mitigate the event. A Hazard Analysis Matrix addressing these different threats has been developed and is provided in Annex 2. The matrix defines the most probable incidents which could render the functions of the UPU International Bureau non-operational. The matrix also defines measures the UPU has taken to mitigate the identified hazards.

2.0 The four scenarios provided below (in terms of severity of impact) provide a framework for activation of the different response levels of the Crisis Management Plan and Business Continuity Plan. For the purpose of this document, it is only realistic that the UPU can institute measures for incidents which result in the consequences listed in *Scenario One – Limited impact emergency* and *Scenario Two – the International Bureau becomes inaccessible.*

3.0 Scenario One – a limited impact emergency

3.1 An incident or event with the International Bureau secretariat or nearby causes an interruption in the normal course of business for a short period of time.

3.2 This situation may involve the loss of life or casualties and might render some of the International Bureau unusable. It may be a residual impact from the failure of part of the city of Berne's infrastructure or a natural disaster.

3.3 This scenario assumes that most staff can still come to work at the International Bureau and that damage to infrastructure or interruption of services is localized or limited. However, this scenario involves the impact of losing the services of key staff, either for a short period or permanently. The expectation is that the International Bureau will be

able to resume most operations within a few days, with most staff and resources in place. There are vital functions that must continue during that short period of time and parts of the International Bureau that must remain available for use to ensure mission critical functions.

3.4 The SEMG and COG meet to manage response and recovery efforts with the International Bureau as set out in section VI above.

4.0 Scenario Two – the International Bureau becomes inaccessible

4.1 An incident or event with the International Bureau or nearby disrupts the normal course of business for an unspecified period of time and calls for the evacuation of the International Bureau secretariat.

4.2 This situation is likely to involve loss of life and assets, and render the International Bureau unusable, while not directly affecting adjacent facilities. The scenario assumes that some staff can come to work and that the city's infrastructure is largely intact.

4.3 The mission critical functions will need to be provided over a more extended period of time from locations in close proximity to the International Bureau site.

4.4 Under this scenario, the SEMG and COG would direct crisis management operations and perform critical business processes from the alternate location specified in Annex 1.

5.0 Scenario Three – Metropolitan Berne becomes unusable

5.1 An incident or events which render the city of Berne unreachable or unusable for an indefinite period of time.

5.2 While some staff might be available to deliver critical functions, most physical infrastructure and support functions would be seriously impaired. Swiss officials are likely to restrict movement into and out of Berne.

5.3 Under this scenario, alternative work sites and staff accommodation may be needed on an interim basis. The loss of the services of key personnel is likely. The continuation of mission critical functions would take place on an interim basis at the direction of the United Nations Office at Geneva. Key staff would be called in to the location designated by the United Nations Office at Geneva, with other staff remaining at home or other locations.

6.0 Scenario Four – Switzerland is the target of a major attack or incident

6.1 A very unlikely incident or event which leads to widespread loss of life and destruction, rendering the country or a major portion of the country uninhabitable for an extended period of time.

6.2 This scenario dictates that most International Bureau functions would have to be resumed, at least for a temporary period of time, at alternative locations elsewhere in the country or world, involving alternate staff or, if feasible, the transfer of International Bureau staff to these locations.

6.3 The SEMG and COG would relocate to a location defined by the United Nations

Headquarters Office. In the event that such relocation is not feasible, it will be necessary to designate members of an alternate SEMG and COG who could function in those locations.

VII. Activation of the Crisis Management Plan

1.0 When a situation or event occurs that has the potential to impact on the operations and/or delivery of mission critical functions of the International Bureau, a crisis exists and the Crisis Management Plan is activated by either the Director General or Deputy Director General.

2.0 The Director of Logistics will be fully involved in the decision making process on the activation of the Crisis Management Plan. In the absence or non-availability of the Director General or Deputy Director General, the Director of Logistics is authorized to activate the Crisis Management Plan. The Logistics Directorate will monitor ongoing incidents and events and will maintain close and regular coordination with Swiss authorities in order to remain fully informed of conditions that may evolve into a crisis impacting the International Bureau. The Logistics Directorate also maintains an up-to-date matrix of all external contact points and liaison contacts, including Swiss authorities, UNDSS and United Nations Headquarters. The UPU electronic Emergency Information System is utilized for communications with member administrations.

3.0 The Logistics Directorate will be responsible for alerting the members of the SEMG and COG to the activation of the Crisis Management Plan. When activation takes place outside normal working hours, the Logistics Directorate will contact members of the SEMG and COG to indicate the location to which they should report. Additionally, the Logistics Directorate will advise the Swiss Permanent Mission, regarding situation and activation of the UPU Crisis Management Plan.

4.0 When a crisis is declared, it is imperative that the members of the SEMG and COG be notified and begins response as quickly as possible. The individuals will be instructed to meet at the designated crisis management venue (Emergency Operations Centre). The location of the primary and alternate Emergency Operations Centre is referenced in Annex 1. However, the location might change from these two locations due to conditions at the alternate site and the impact of the crisis. Members of these groups may be initially directed to assemble at a separate mobilization point until one of the two predefined locations is made operational.

5.0 Once assembled, the Director of Logistics will brief the SEMG and COG on the preliminary assessment of the event. One of the first tasks of COG members will be to establish a line of communication with their chain of command in their directorates/units to ensure that their internal crisis plans have been activated, to direct them to begin assessment of the impact of the event, and to alert their principal vendors for possible immediate requests for assistance. Each COG member will represent their department with full decision-making powers. The Director of the Executive Office (DCC), Head of Cabinet and Director of Logistics will ensure that the Swiss authorities and United Nations Headquarters are aware of the crisis and alert them to possible requests for assistance. When preliminary assessments are completed, the SEMG will meet to take policy decisions, review problems and questions that may arise in the near term.

6.0 **General Operating Principals for the SEMG and COG members:**

6.1 Reinforce centralized information flows and decision making throughout the duration of the crisis.

6.2 Ensure that all information for external distribution is released only with the clearance of the SEMG.

6.3 Assign a priority order in which crisis-related tasks are to be addressed. (For example, re-establishing power to the IB, telephone connections, etc...)

6.4 Members of the COG will perform and safety and operational assessment to ensure that either the International Bureau or the Alternate Location for the Business Continuity functions can operate safely and has the necessary equipment to support the core personnel. After these assessments, the SEMG will determine when the Business Continuity Plan will be activated.

6.5 A generic Emergency Response Checklist is provided as Annex 3. This document can be used as a general guide in regard to the actions which should be performed to manage the crisis. The checklist contains a contact list for critical staff, suppliers, UPU members or international organizations, and other relevant individuals. The checklist also contains an Event/Action Log Sheet to record activities performed by the SEMG or COG.

VIII. Activating the Business Continuity Plan – Critical Business Processes

1.0 After the decision by the SEMG that the International Bureau, the Alternate Location or the remote access options are suitable to support the operations of the core staff, the Business Continuity Plan will be activated. Each Directorate and Unit has previously identified the critical business processes they perform.

2.0 The Critical Business Processes performed by the following Directorates and Units are included in this document:

- The Director General and Cabinet (including DCC)
- Communication (Internal and External)
- Operations and Technology Directorate
- Director of Legal Affairs and Ethics Bureau
- Directorate of Markets
- Finance Directorate
- Logistics Directorate
- Human Resources Directorate
- Development Cooperation Directorate
- EMS Unit
- Postal Technology Center

3.0 The incident will most likely result in limited staff and equipment resources. Therefore, it will be necessary to prioritize which Critical Business Processes are performed. A predefined Priority List of Critical Business Processes is provided in Annex 4. This document should only be used as a reference guide to direct resources during an incident.

4.0 Each Directorate or Unit has developed Standard Operating Procedures for each critical business process they perform. These procedures are attached to this document as Annex 5. These procedures detail the critical employees and required resources to perform these functions. For each critical business process the responsible directorate or unit must ensure that the information provided in Annex 5 is current.

IX. Scope and Objectives of the Business Continuity Plan

1.0 The Business Continuity Plan covers a very limited number of scenarios under which it would be implemented. They scenarios are as follows:

1.1 The UPU International Bureau is accessible/operational with the core staff performing the critical business processes.

1.2 The UPU International Bureau is not accessible/operational. The core staff performs the critical business processes at the Alternate Site listed in Annex 2.

1.3 The UPU International Bureau and the Alternate Site are not accessible/operational. The core staff performs the critical business processes remotely using laptops, telephones, and other equipment provided by the UPU.

2.0 As determined by the Business Impact Analysis, an overview of the Critical Business Processes is listed in Annex 4.

Annex 1 Locations of Emergency Operations Centre (EOC) and Continuity of Operations Site

Primary (EOC) Site
The Rowland Hill conference room at the UPU International Bureau located at Weltpostrasse 4, CH 3015 Bern, Switzerland will be utilized as the primary site of the Emergency Operations Centre (EOC) in the event of a major incident or disaster.

Alternate (EOC) Site (currently, alternate locations are still being evaluated)

In the event that the UPU International Bureau is not accessible, the SEMG and the COG will meet in the XXXX room at XXXX facility in Bern. The address of this facility is:

Address
Telephone: +41 31 xxx xxxx
FAX: +41 31 xxx xxxx

Directions: <provide directions>

Continuity of Operations Site

Primary Continuity of Operations Site
The UPU International Bureau located at Weltpostrasse 4, CH 3015 Bern, Switzerland will be utilized as the primary site to perform critical business processes of the UPU in the event of a major incident or disaster. The COG will notify core personnel (Business Continuity Team) to report to the site upon assessment of the incident.

Alternate Continuity of Operations Site (currently, alternate locations are still being evaluated)
In the event that the UPU International Bureau is not accessible, the COG will notify the core personnel (Business Continuity Team) to meet in the XXXX room at XXXX facility in Bern. The address of this facility is:

Address
Telephone: +41 31 xxx xxxx
FAX: +41 31 xxx xxxx

Directions: (Provide driving and mass transit directions)

Remote Operations
In the event that the UPU International Bureau and the Continuity of Operations Alternate Site is not available, the functions of the Business Continuity Team will be performed remotely. Access and communications will be developed by the Logistics Directorate.

Annex 2 Hazard Analysis Matrix

Risk Matrix Score

A = HIGH Likelihood and HIGH Impact

B = LOW Likelihood and HIGH Impact

C = HIGH Likelihood and LOW Impact

D = LOW Likelihood and LOW Impact

Hazard	Impact	Mitigation in Place	Mitigation possible	Risk Matrix Score
Flooding	• Limited access to IB • Possible damage to IT • Damage to infrastructure		• Installation of pump	**D**
IT Failure	• Loss of services • Loss of productivity	• Back-up system		**B**
Loss of electricity	• Loss of service • Building less secure • Loss of productivity	• Emergency generator		**B**
Fire	• Limited access to IB • Damage to infrastructure	• Fire Detection and suppression equipment		**B**

Annex 3 Sample Emergency Response Checklist and Contact Details

1. Emergency Response Checklist

Start a log of actions taken ☐
Liaison with Emergency Services ☐
Identify any damage ☐
Identify functions disrupted ☐
Convene SEMG and COG ☐
Liaison with the City of Berne, UNOG or Swiss Authorities ☐
Provide information to staff ☐
Decide on a course of action ☐
Communicate decisions to staff and key stakeholders ☐
Conduct communications ☐
Evaluate safety and operational capabilities to support BCP ☐
Activate BCP ☐

2.0 Contact Details

2.1 Core Staff Contact Details

Name	WorkPhone	HomePhone	Mobile	Email

2.2 Key Suppliers and Vendors

Name of Supplier or Vendor	Material or Service	Telephone	Alternate Telephone and Fax	Email

2.3 UPU Members/Stakeholders and International Organizations

Name of Stakeholder	Relationship	Telephone	Alternate Telephone and Fax	Email

2.4 Utility Companies

Utility	Company	Telephone	Alternate Telephone and Fax	Email

2.4 Insurance and Financial Contacts

Service	Company	Telephone	Alternate Telephone and Fax	Email

3.0 Action and Expense Log

Date/Time	Decision/Action Taken	By Whom	Costs Incurred

Crisis Management and Business Continuity Plan
Universal Postal Union

Annex 4 List of Critical Business Processes

1. DRH – Salary payments for regular staff interpreters and other short term contract staff
2. DRH – Organization of Missions
3. DRH – Communications with external partners such as Insurance companies and Swiss Permanent Mission
4. DCC – Staff communications (Health and Safety issues)
5. DCC –External Communications
6. DCC - Operations of the DG and VDG
7. DAJ – Review of essential contracts and documents
8. DOT – Operation of EmIS
9. DOT – Organization of CEP and other reunions
10. DOT – Support for QS Programme
11. DOT.EMS – Broadcast messaging (e-mail)
12. DOT.EMS – EMS on-line Ops Guide and website
13. DOT.EMS – Delivery Validation
14. DOT.EMS – Performance reporting
15. DOT.PTC – PTC Telephone Support
16. DOT.PTC – PTC Process and System Monitoring
17. DOT.PTC – PTC Development and Deployment of Applications
18. DOT.PTC – PTC Server Maintenance and Back-up Process
19. DL.PSGC – Maintain IB Mail Services
20. DL.PSGC – Maintain IB Telephone Services
21. DL.PSGC – Maintain IB Computer Network
22. DL.PSGC – IB General Building Services
23. DL.PDO – Functions of Typists
24. DL.STFR – Functions of Translation Services
25. DFI – Functions of UPU Clearing
26. DFI – Salary / pension payments
27. DFI – Payments and cash management
28. DFI – Accounting

29. DFI – Providence scheme
30. DOT.ADU – Telephone and email support for PostCode clients and data suppliers
31. DOT.ADU – Addressing database maintenance and data delivery process to Licensees
32. DCDEV – Consultant Missions
33. DCDEV – Training Missions
34. DCDEV – Purchase of Material for projects
35. DCDEV – Administrative actions for regional consultants and experts
36. DDM – International Reply Coupons
37. DDM – Stamp distribution
38. DDM – WADP Stamp Numbering

Annex 5 Standard Operating Procedures for Critical Business Processes

<Template to be completed for each Critical Business Process>

Function 1 - <provide business name, e.g. Payroll and a brief description of the business function the IB is required to resume or recover>

Function 1 - <provide business name> Business Continuity Team (BCT)
<Define the members of BCP Team for this function. For each team member provide the following information.>

Role or Responsibility: <Describe the responsibilities of this team member. (e.g. - Team Leader - responsible for coordinating all team activities and reporting status to the SEMG or COG)>

Name: <The name of the team member>
Address: <If all telecommunications are out of service or tied up, it may be necessary to contact this team member in person by visiting their residence.>
Contacts: <List all possible contacts for this team member and clearly identify each. Include area codes if long distance calls are required.
Office Tel: <Business telephone number>
Home Tel: <Home telephone - include city code if applicable).>
Cell Phone: <Cellular telephone - include city code if applicable).>
Fax: <Fax number - include city code if applicable).>
E-Mail: <Business and personal E-mail address, if applicable).>
<Add any other contact points that may be appropriate.>

Alternate Name: <The name of the alternate or backup team member in the event that the primary member is unavailable.>

Address: <As for the primary member.>
Contacts: <As for the primary member.>

Function 1 - <provide business name> Recovery Procedure
<A brief description of the recovery procedure. Describe the level of service being recovered (i.e. - full service, basic service, shutdown of operations, etc.)>

Function 1 - <provide business name> Recovery Time Objective (RTO)
<RTO is defined as the maximum acceptable length of time that can elapse before the lack of a business function severely impacts the business entity. State your Recovery Time Objective for this function and the level of service to be attained within the RTO. You may have multiple levels of service and RTO's. (e.g. - 50% resumption of service within 4 hrs, 80% within 8 hrs, 100% within 2 days)

Function 1 - <provide business name> Recovery Location
< Describe the location where the business resumption/recovery procedures will take place. Give address, telephone number and detailed directions on how to get there. If this activity is to take place in a pre-arranged area of a common location, specify where this area is. >

Function 1 - <provide business name> Dependencies

<Describe dependencies this recovery process has on other departments or business units. (e.g. - you may require access to special facilities controlled by another department; you may require a list of suppliers from IT; you may be dependent on an updated employee telephone list being deposited by human resources at the EOC each month.)>

Function 1 - <provide business name> Other Considerations
<If applicable, describe any other factors that should be taken into consideration or that might affect the recovery process. (e.g. - this process could involve a huge financial outlay - this might require pre-approval.)>.

Function 1 - <provide business name> Recovery Steps - Summary
<Provide a simple list (i.e. - one line per step) of the steps involved in this procedure. For example - see the following:

Example below

- ❑ Step 1 – Contact Business Continuity team members and arrange for a meeting.
- ❑ Step 2 – Business Continuity team meets and reviews plan.
- ❑ Step 3 – Contact vendor XXX.
- ❑ Step 4 – Contact XXX staff and set up information meeting.
- ❑ Step 5 – Review staffing requirements.
- ❑ Step 6 – Meet with vendor staff and inform of situation.
- ❑ Step 7 – Visit vendor warehouse and order XXXX.
- ❑ Step 8 – Contact shipping companies and inform them of new pickup and drop-off location.
- ❑ Step 9 – Contact purchasing and stop delivery of identified products.
- ❑ Step 10 – Contact sales to instruct customers of situation.
- ❑ Step 11 – Meet with warehouse staff and review operating procedure.
- ❑ Step 12 – Run a test order through the system.
- ❑ Step 14 – Order additional shipping supplies.
- ❑ Step 15 – Contact IT and determine when computer services will be restored.
- ❑ Step 16 – Arrange for implementation of XXX.

Resource Requirements for Recovery:

Time	No. of staff	Location/Space	Resources required	Data required
First 24 hours				
24 – 48 hours				
Up to 1 week				
Up to 2 weeks				

2.8. Acil durum hazırlık

Sayfaya Geri Dön

CONTINUITY OF OPERATIONS PLAN

Example Critical Facility

February 20XX

RESTRICTED INFORMATION

The information contained in this document is for OFFICIAL USE ONLY and is protected by the Privacy Act. It is to be used only to contact essential personnel in response to an emergency situation. Unauthorized use of this information may constitute an invasion of privacy.

APPROVALS

By their signatures below, the following officials certify that they have read this Continuity of Operations Plan (COOP) and fully understand the business resumption procedures to be followed in an emergency affecting the facilities and employees for which they are responsible.

Approved: _____ Date _____

Vice President

Approved: _____ Date _____

Manager, Operations Support

Primary/Secondary Threats at Critical Facility

HAZARD/THREAT	VULNERABILITY		
	Low	**Med**	**High**
Primary Hazards/Threats:			
Hurricane/Tornado/Windstorm	X		
Terrorism/Weapons of Mass Destruction	X		
HAZMAT release	X		
Crime	X		
Transportation accidents	X		
Bomb (threat)		X	
Flooding	X		
Fire/Wildfire		X	
Power failure/interruption		X	
Civil disturbance	X		
Health hazard/disease		X	
Communication interruption	X		
Earthquake		X	
Volcano	X		
Tsunami	X		
Secondary Hazards/Threats			
Prohibited access to the facility		X	
Smoke damage	X		
Hazards/threats to adjacent facilities	X		
Structural damage		X	
Communications lines down		X	
Loss of electrical power & blackouts		X	
Water damage	X		
Ruptured gas main		X	
Air or water contamination		X	
Explosion		X	
Building collapse		X	
Trapped persons		X	
Chemical release	X		

SECTION 1
INTRODUCTION AND PLAN OUTLINE

1.0 INTRODUCTION

This plan documents the procedures for ensuring continuity of operations (COOP) for a critical facility. It will enable the office to resume minimum essential operations within 12 hours of an emergency, with or without warning, and to sustain emergency operations for up to 30 days.

1.1 INTENDED AUDIENCE

The intended audience of this COOP Plan is the critical facility managers and staff under the direction of the Emergency Management Team. **This plan is to be used by this critical facility only**. A separate COOP plan has been prepared for other locations as necessary.

The Vice President, (or designee) will have overall responsibility for this COOP plan. The security group will be responsible for coordinating with all functional departments in maintaining the accuracy and ensuring the COOP Plan is current.

Each of the Essential Staff will be provided with a current copy of this plan.

1.2 APPLICABLE REGULATIONS

In accordance with security standards set by the Universal Postal Union and local government agencies these emergency plans were developed to meet essential defense and civilian needs during any level of national security emergency.

1.3 OBJECTIVE

This COOP plan is intended to ensure the critical facility is prepared to accomplish the following:

- Provide essential services to the operations of XYZ post and installations in the event of a wide range of potential emergencies.
- Protect essential equipment, records (operating, legal, and financial), and assets.
- Reduce or mitigate disruptions to operations by minimizing the loss of resources and by providing timely and orderly recovery from an emergency and the resumption of full service.

The COOP plan will be used to assist in all phases of Emergency Management: Mitigation, Preparedness, Response and Recovery.

1.4 PLAN OUTLINE

This COOP Plan organized into sections to help you locate information and instructions.

SECTION 2
COOP MITIGATION AND PLANNING

2.0 INTRODUCTION

This Section will provide instruction on policies and procedures needed do prepare for implementation of the COOP plan, as well as provide a general line of succession in the event the upper management is not available at the time of the emergency.

2.1 SUCCESSION PLANNING

Essential functions will proceed without interruption regardless of the availability of any individual. During any period in which the top position of the facility is vacant, the official highest on the following list (who is not sick or absent) shall perform the duties.

LINES OF SUCCESSION	
Order (Title)	**Name**
Vice President or Top Position	
First Replacement	
Second Replacement	
Third Replacement	

Table 2-A

2.2 COOP DECISION TEAM

As soon as possible after an incident that requires an evacuation, the Manager will activate the COOP Team. The COOP Team roster is presented below. It should be noted that, while each member of the COOP team provides input on the emergency situation, the final decision to implement the COOP lies with the top position.

COOP TEAM MEMBERS		
Title	**Primary**	**First Alternate**
Top Position		
Manager, Operations		
Manager, Finance		

Table 2-B

2.3 COOP SITES

In the event that the COOP plan is activated, the Functional areas within the critical facility will report to the locations identified in the table below. The table below also lists essential equipment, materials, data, databases, and software that are to be pre-positioned at the

alternate COOP locations. These essential items include equipment and materials that would be required by the staff to accomplish their various tasks during the emergency and immediately afterward. Common items such as printer paper etc. should not be included here because one would expect to be able to find them already there. Directions are in Appendix 7-2

2.

Functional Area: Top Office	
Functional Area Manager	
Employees in Unit	2
Relocation Site	
Type of Connectivity Available	Fully Operational
Workstations needed	2
Equipment Needed	
Lap Top/Blackberry	2

Functional Area: Operations Office	
Functional Area Manager	
Employees in Unit	2
Relocation Site	
Type of Connectivity Available	Fully Operational
Workstations needed	2
Equipment Needed	
Lap Top/Blackberry	2

Table 2-C

Functional Area: IT Support	
Functional Area Manager	
Employees in Unit	12
Relocation Site	
Type of Connectivity Available	Fully Operational
Workstations needed	12
Equipment Needed	

Lap Top/Blackberry	12

Functional Area: Human Resources	
Functional Area Manager	
Employees in Unit	12
Relocation Site	
Type of Connectivity Available	Fully Operational
Workstations needed	12
Equipment Needed	
Lap Top/Blackberry	12

2.4 MINIMUM ESSENTIAL FUNCTIONS

Prior to an emergency event, the Critical Office has identified essential functions it must perform during an emergency. Although the Critical Office may perform any or all of its other normal functions during the emergency, these functions, known as the minimum essential functions, must be accomplished. These functions may include retrieving important documents, supplies or plans.

A list of minimum essential functions and the lead contact responsible for ensuring the function is completed is in the table below.

MINIMUM ESSENTIAL FUNCTIONS	
FUNCTIONS	**RESPONSIBLE PARTY**
Manage Emergency/Contact Headquarters	
Notify Other Mgrs, Activate Alternate Facility Operations Provide Daily Status Reports	Manager, Operations Support
Coordinate Emergency Mgmt Issues	Manager, Security and Safety
Coordinate Security Issues at Primary And Alternates Sites	Manager, Security and Safety
Provide Equipment & Hardware Support Provide Software & Directory Support	Manager, Maintenance

Process Financial Transactions Receive/Deliver Payroll Documents Collect Time/Attendance Ensure Cash is Available for Payments	Manager, Accounting
Oversee Express Mail Operations	Express Mail Program Analyst
Recruiting/Selecting/Deploying Personnel Providing Access to Records	Manager, Human Resources
Employee Communication	Manager, Labor Relations
Promoting Employee Health/Safety Coordinating First Responders	Manager, Safety
Provide Employee Communication Manage News Media	Communications

2.5 TELEPHONE AND FAX FORWARDING

This table lists the telephone and fax numbers to be forwarded during COOP implementation and the corresponding proposed temporary numbers at the primary COOP site.

Telephone and Fax Forwarding Numbers

WA Functional Office	Current Phone/FAX	Primary COOP Site (Midway) Phone/FAX
Vice President		
Manager, Operations Support		
Manager, In-Plant Support		
Manager, Delivery Programs		
Manager, Maintenance Support		
Manager, Finance		
Manager, Human Resources		
Mgr, Public Affairs/Communication		

Table 2-E

SECTION 3
COOP RESPONSE ACTIONS

3.0 INTRODUCTION

This section details the response actions that will be taken in the event that an emergency at or near the Critical Office results in a decision to activate the COOP.

3.1 ACTIVATION

During the initial stages of an emergency requiring relocation, or at the time specified by the Manager, Critical Office must move essential staff members to its alternate site(s) and commence minimum essential operations. This phase requires the following steps:

3.1.1 ACTIVATE FUNCTIONAL MANAGERS

The Vice President, with assistance from staff, will notify all Functional Mangers of the COOP activation. Communications from the Manager, Operations Support to the Functional Managers shall consist of the following:

> "The Critical Office has initiated its COOP Plan. You are to report to your Functional Office's selected deployment site as soon as possible."

FUNCTIONAL MANAGER CALLING TREE		
FUNCTIONAL AREA	**MANAGER**	**CONTACT NO.**
Vice President, Area Operations		Work: Cell: Home:
VP Assistant		W: C:
Operations Support		W: C:
Mgr, Transportation		C: H:
Manager, Accounting		W: C: H:
Human Resources		W: C:
Public Affairs & Communications		W: C: H:

3.1.2 ACTIVATE STAFF

Once notified by the Manager, it will be each Functional Managers responsibility to notify and deploy their direct staff. Functional Managers will use the chain of supervision to make additional notifications to their staff and inform them of the COOP Activation.

3.1.3 PERFORM MINIMUM ESSENTIAL FUNCTIONS

Once the COOP plan has been activated for the facility minimum Essential Functions identified in Section 2.4 must be carried out.

3.1.4 GET DEPLOYMENT SITE OPERATIONAL

Within 12 hours of the emergency, deploying personnel will occupy their assigned work space, obtain prepositioned material, upload prepositioned software, and download prepositioned data and databases (see Section 2.3 for a list of these materials).

3.1.5 REPORT CLOSURE AND OPERATIONAL STATUS.

Once alternate site operations are established, the Office will provide the following minimum information to internal elements, and other agencies as appropriate for further instructions on the actions identified below.

- Locations where the Office has established alternate sites
- Status of communications
- Any business functions that will be interrupted or suspended
- Anticipated duration for operating from the alternate sites
- Anticipated duration of any business function degradation.

SECTION 4
COOP RECOVERY ACTIONS

4.0 INTRODUCTION

Once the Office has activated its functions at the alternate site(s), it must be able to sustain operations for up to 30 days. Workload will be scaled back to perform at least minimum essential functions. All other work will be set aside for the next 30 days pending full restoration of the current location or occupation of an interim site while awaiting full restoration. To the maximum extent possible, these minimum essential functions will be performed using the same processes and systems normally used. A second major effort during this 30-day period will be to develop plans on how to operate beyond the initial 30 day period. In addition to performing these functions, the Office will develop plans and schedules to phase out the alternate site operations and return activities, personnel, records, and equipment to the Office or another temporary or permanent site when the emergency is terminated.

4.1 RESUMPTION OF NORMAL OPERATIONS

Restoring normal operations at the Office requires detailed planning. The two aspects of restoration are 1) reoccupying the old office (or occupying a different one) and 2) resuming normal business operations. Specific activities associated with termination and resumption of normal operations includes the following:

- Informing all personnel, including non-deployed personnel, that the emergency no longer exists and providing instructions for the resumption of normal operations.
- Supervising the orderly return to the office or to other temporary or permanent facilities.
- Conducting a critique of COOP plan procedures and effectiveness as soon as possible to identify areas for improvement and to develop plans for implementation.
- Terminating or revising work-forwarding instructions.
- Informing clients and stakeholders of the Office new location, telephone numbers, etc., if applicable.

During an emergency, some functions may be performed differently than during normal operations. For example, manual record keeping may temporarily be required in areas that normally rely on automated systems. Restoration of normal business practices requires updating systems and files to incorporate essential elements created during the emergency.

SECTION 5
RESPONSIBILITIES AND TRAINING

5.0 PERSONNEL RESPONSIBILITIES

Specific responsibilities associated with this COOP Plan are:

The Manager is responsible for the following:

- Maintaining a viable COOP plan
- Determining when to deploy to an alternate site in the event of an emergency.

The Manager, Operations Support is responsible for the following:

- Managing the review of the COOP plans in January and June of each year
- Updating the telephone trees semi-annually
- Updating the telephone and fax forwarding lists semi-annually
- Updating the e-mail forwarding lists semi-annually
- Conducting a review of essential materials, data, databases, and software in the pre-positioned location.
- Initiating work forwarding
- Reporting closure at the deployment site and status
- Notifying stakeholders of the resumption of normal services

The Functional Area leaders assigned to the Office are responsible for the following:

- Executing their portion of the COOP plan
- Pre-positioning and refreshing essential materials, data, databases, and software at an alternate site(s)
- Revising the deployment roster as needed
- Providing semi-annual input for updating the telephone contact lists
- Providing semi-annual input for updating the telephone and fax forwarding lists
- Providing semi-annual input for updating the e-mail forwarding lists

Employees are responsible for the following:

- Keeping their home telephone, cell phone, and pager numbers current with their Functional Manager
- Deploying to the appropriate site when notified

5.1 PLAN UPDATES

The Manager, Operations Support or designated representative will manage the review of the COOP plan and updating as scheduled (January & June) or as needed.

PLAN UPDATE SCHEDULE	
ITEM	**UPDATE MONTH**
Deployment roster	**January & June**
Review of essential materials, data, databases, and software at alternate locations	**January & June**
Emergency Telephone Trees	**January & June**
Telephone, fax forwarding list and email addresses	**January & June**

TABLE 5-1

5.2 TRAINING, TESTING, AND EXERCISES

Annual COOP Awareness training/orientation will be conducted to assure the readiness of all Office personnel. The purpose of this training is to prepare Office personnel to institute emergency operations at an alternate facility, to use equipment and procedures and to work with individuals with whom they have little contact during normal day-to-day operations.

The alert notification process described in this COOP Plan will be reviewed semi-annually.

Exercises will be conducted for the purpose of validating elements, both individually and collectively, of this COOP Plan. A COOP exercise, whether it is a tabletop simulation, series of drills, a functional exercise, or a full-scale exercise, will be conducted annually. Lessons learned from each exercise will be incorporated into a remedial action plan for the January COOP Plan update.

SECTION 6
DISTRIBUTION

Distribution of the COOP plan will be available on the intranet and may be downloaded onto an Encrypted flash drive.. Distribution of the entire plan, which may contain classified or sensitive information, will be restricted to essential personnel governed by a need-to-know.

All COOP plans are considered internal decisional documents with national and domestic security protections afforded under applicable statutes.

Primary List (full COOP plan)

- All Managers

SECTION 7 - APPENDICES

7-3 EOC locations & directions &24/7 coverage

Emergency Operations Center (EOC) is the physical location that serves as the USPS' single focal point for the management of information, decision-making and resource support/allocation during the entire disaster management and recovery process. In the table below, identify primary and alternate EOC locations that may be activated during an emergency.

The EOC should be pre-stocked with supplies and equipment to allow for quick response to and effective management of the emergency. In the table below, identify type and quantity of available equipment and the EOC location where the equipment can be found.

EMERGENCY EQUIPMENT AND SUPPLIES LIST						
Equipment	**Quantity**	**Location(s)**				
		EOC #1	**EOC #2**	**EOC #3**	**EOC #4**	**EOC #5**
ICS Vests	1-Sets					
Pens	10-Boxes					
Highlighter	10-Sets					
Steno Notebooks	1-Case					
Copy Paper	1-Case					
Bull Horn	1-Each					
Dry Erase Markers	5-Sets					
Hole Punch	5-Each					
File Folders	2-Boxes					
Blank CD-ROMs	100-Ea					
Advanced First Aid Kit	1-Kit					
Food & Water	1 Week					
Facility Drawings						
Thomas Guide	5-Each					
Large Area Maps (wall)	5-Each					
Hand Held Radios	20-Each					
Radio Interface System	1-Each					
TV/VCR	3-Each					

2.9 Tehlikeli Madde Eylem Planı

Sayfaya Geri Dön

HAZMAT RESPONSE PLAN

WHAT IS A HAZARDOUS MATERIAL RELEASE?

A variety of hazardous chemicals are routinely used in day-to-day facilities operations (e.g., paints, inks, solvents, cleaners). In addition, certain kinds ofchemicals or infectious substances are considered mailable (in limited quantities),and may be found in parcels that have entered the mailstream. Occasionally,hazardous materials may spill, leak, or otherwise be released into theworkplace or the environment. Such events can be categorized as being eitherincidental releases or emergency releases.

An Incidental Release is a minor or non-emergency event that presents limitedrisk to the health and safety of employees. Such eventsare typically small in quantity, have little potential for humanexposure, and involve materials of low toxicity. Still,incidental releases must be taken seriously. Any hazardousmaterial release has the potential to evolve into a muchmore serious emergency if not confined quickly and respondedto appropriately.

An Emergency Release is a more significant event and can result in major risksto the health and safety of employees and customers, aswell as damage to the environment and property.Such events constitute real or threatened emergency situations,and can involve fire, explosion, or severe chemicalexposure. Generally, a coordinated response from an outsideemergency response organization (e.g., fire department,hazardous materials response team) is required tosafely contain, cleanup, or otherwise respond to an emergencyrelease.

In the event of a hazardous material release, it is important that trained personnelare able to quickly assess and determine whether an incidental or emergencyrelease is occurring. The ability to distinguish between these two categories ofreleases will largely determine what response procedures should be followed.When in doubt, check with your supervisor, safety personnel, or hazmat trained specialists. Play it safe and err on the side of safety.

Who May Respond

Only personnel who have received HAZMAT training are qualifiedto respond to spills, leaks, and other incidental releases of hazardous chemicalsor infectious biological materials. Personnel who have received trainingare only qualified to respond to spills, leaks, and other incidental releases ofinfectious biological materials. If you have not undergone training at, you should not become involved in responding to a hazardouschemical or infectious substance release. If you should notice a leakingpackage, your only duty is to immediately notify a trained HAZMAT responder that a potential hazardous chemical or infectious substance releasehas occurred.

Procedures to be Followed

Following appropriate emergency response procedures quickly and correctly canreduce injuries, help save lives, and prevent damage to property and theenvironment. Based on your level of training, the following general responseguidelines should be followed if you witness or are called to respond to a hazardousmaterial release.

1. Consider your and your co-workers safety.
2. Contact Supervisor who will contact “HAZMAT trained” personnel.
3. Isolate the spill if it is safe to do so.
4. Identify the hazardous materials released if it issafe to do so.
5. Determine if the release is incidental or emergency.

If Incidental Release:

- Determine safe clean-up and rewrap/disposal measures.
- Determine what protective equipment and other hazard control measures are needed.
- Determine if evacuation is necessary.

If Emergency Release

- Contact management, as needed, to evaluate the need for an outside response agency (hazmat team) or spill contractor.
- Follow actions indicated in the facility emergency response plan.

Provide the outside Emergency Response team with pertinent information, including:

- Your name and the location of the release.
- Estimated amount of released material.
- Identity of material (chemical or trade name or description).
- Known hazards to workers or the environment.
- Conditions at the scene (fire, injuries, or property damage).
- Details about the nature of release (e.g., whether vapors are escapinginto the air or the spill is spreading).

These response guidelines are applicable to hazardous chemical or infectioussubstance incidents that occur in the mailstream, as well as part of routine facilityactivities. The order in which you carry out the duties listed above will depend onthe specific circumstances of each incident. Always remember that your responsibilitiesto respond to an emergency do not involve risking your life!

4.2. Avustralya Tehlikeli Posta Dokümanı

Sayfaya Geri Dön

AUSTRALIA POST

DANGEROUS GOODS BANNED FROM THE POST

DANGEROUS GOODS CLASSIFICATION

DANGEROUS GOODS, HAZARD CLASS AND ILLUSTRATIONS OF HAZARD LABEL	DEFINITION	COMMON EXAMPLES
CLASS 1	EXPLOSIVES	Flares, safety cartridges, primers cap type, ammunition, caps for toy pistols, fireworks
CLASS 2.1	FLAMMABLE GAS GASES UNDER PRESSURE, WHEN MIXED WITH AIR IN CERTAIN PROPORTION BECOMES FLAMMABLE	Aerosols, L.P gas, butane cigarette lighters
CLASS 2.2	NON-FLAMMABLE, NON TOXIC GASES UNDER PRESSURE, MAY BE ASPHYXIANT OR CONTRIBUTE TO COMBUSTION OF OTHER MATERIALS	Cylinders of compressed air, nitrogen, carbon dioxide, fly sprays, fire extinguishers
CLASS 2.3	TOXIC GAS GASES KNOWN TO BE TOXIC OR CORROSIVE TO HUMANS	Chlorine gas, insecticides and nitric oxide
CLASS 3	FLAMMABLE LIQUID LIQUIDS THAT GIVE OFF A FLAMMABLE VAPOUR BELOW A CERTAIN TEMPERATURE & THAT COULD IGNITE IF EXPOSED TO AN IGNITION SOURCE	Some essential oils, methylated spirits, petrol, paints, white spirits, most perfumes, finger nail polish
CLASS 4.1	FLAMMABLE SOLID READILY COMBUSTIBLE SOLID THAT MAY CAUSE OR CONTRIBUTE TO A FIRE THROUGH FRICTION	Safety matches sulphur, barbeque starters
CLASS 4.2	SPONTANEOUSLY COMBUSTIBLE SUBSTANCES	Phosphorus, other powders, sodium hydrosulphite
CLASS 4.3	DANGEROUS WHEN WET SUBSTANCES WHICH IN CONTACT WITH WATER EMIT FLAMMABLE GASES, OR BY INTERACTION WITH WATER ARE LIABLE TO BECOME SPONTANEOUSLY FLAMMABLE OR GIVE OFF FLAMMABLE GASES IN DANGEROUS QUANTITIES	Sodium metal, other metal powders, magnesium alloys
CLASS 5.1	OXIDIZING SUBSTANCE READILY YIELDS OXYGEN AND STIMULATES FIRE IN OTHER MATERIALS	Some pool chemicals, bleaches, nitric acid, hair dyes
CLASS 5.2	ORGANIC PEROXIDE REACTS DANGEROUSLY WITH OTHER SUBSTANCES CAN BE READILY IGNITED BY IMPACT OR FRICTION AND MAY BURN RAPIDLY	Fibreglass repair kits
CLASS 6.1	TOXIC SUBSTANCES LIQUIDS OR SOLIDS WHICH ARE DANGEROUS IF INHALED, SWALLOWED OR ABSORBED THROUGH THE SKIN. INCLUDES SOME MEDICINES	Many agricultural chemicals - herbicides and insecticides - chloroform
CLASS 7	RADIOACTIVE MATERIAL EMIT RADIATION WHICH CAN BE HARMFUL TO YOUR HEALTH. RADIOACTIVE MATERIALS CANNOT BE DETECTED BY ANY OF THE HUMAN SENSES (SIGHT, TOUCH, HEARING, SMELL, TASTE)	Medical isotopes, scientific samples, some smoke detectors
CLASS 8	CORROSIVES MAY CAUSE SEVERE DAMAGE TO LIVING TISSUE (YOUR SKIN) OR DAMAGE OTHER GOODS	Battery acid, spirits of salts, sanitizing agents, mercury
CLASS 9	MISCELLANEOUS DANGEROUS GOODS SUBSTANCES THAT MAY PRESENT A DANGER (NOT COVERED BY OTHER CLASSES) TO HUMAN HEALTH OR OTHER ARTICLES	Dry Ice, batteries, life saving appliances - may contain dangerous goods such as matches and flares
OTHER ITEMS NOT PERMITED	MAGNETIZED MATERIAL	Magnets
OTHER ITEMS NOT PERMITED	CRYOGENIC LIQUID CAN BE AN ASPHYXIANT WHEN RELEASED INTO ATMOSPHERE IN CONFINED AREA. DIRECT CONTACT WITH SKIN MAY RESULT IN COLD BURN	Containers for carriage of semen used in animal or human reproduction programmes

4.3. USPS Uluslararası Tehlikeli Posta Dokümanı

Sayfaya Geri Dön

PROHIBITED in INTERNATIONAL MAIL
Dangerous Goods Warning Labels

MAILABLE to INTERNATIONAL
(Under Certain Conditions)

Infectious substance
Mailpieces containing specific types of infectious substances (Class 6, Category B) are acceptable in international mail subject to the provisions of DMM 601.10.17 and IMM 135.

Radioactive substance, excepted package
Mailpieces containing Class 7 radioactive materials are acceptable in international mail subject to the provisions of DMM 601; Publication 52, *Hazardous, Restricted, and Perishable Mail;* and IMM 135.

4.1.1'den 4.1.7'ye kadar USPS Güvenlik Afişleri

Sayfaya Geri Dön

POSTES CANADA POST
De partout... jusqu'à vous

Marchandises dangereuses
Articles à ne pas envoyer

Marchandises dangereuses

Il est interdit d'envoyer des marchandises dangereuses dans le courrier. Bon nombre d'articles du quotidien, tels que ceux qui sont présentés, pourraient être des marchandises dangereuses et occasionner des accidents graves s'ils sont expédiés.

Il vous incombe de veiller à ce que votre colis ne contienne aucune marchandise dangereuse. **Grâce à votre collaboration, il est possible de prévenir des accidents.**

Étant donné qu'il est interdit d'envoyer des marchandises dangereuses dans le courrier, vous pourriez être tenu responsable si un accident survient.

Pour obtenir plus de renseignements, veuillez communiquer avec le Service à la clientèle au **1 800 267-1177.**

NOTA: *Les exemples présentés sont des exemples courants d'articles interdits et ne représentent pas une liste exhaustive des marchandises dangereuses. Si vous voulez savoir si vous pouvez expédier un article précis, veuillez composer le numéro du Service à la clientèle.*

Pour obtenir plus de renseignements, veuillez communiquer avec le Service à la clientèle :

Sans frais : 1 800 267-1177
ATS/ATM : 1 800 267-2797

Batteries au lithium

Bien qu'il soit sécuritaire de transporter des batteries au lithium avec vous, leur expédition en tant que colis comprend des risques sérieux *(ces risques s'appliquent aux petites batteries au lithium, telles que celles utilisées pour l'alimentation des téléphones cellulaires et des ordinateurs portatifs).*

La surchauffe ou le court-circuit d'une batterie pendant le transport pourrait avoir de conséquences désastreuses. Postes Canada accepte les batteries au lithium sous réserve de certaines conditions.

Veuillez vous assurer de vérifier les critères d'admissibilité des batteries au lithium de Postes Canada en consultant la section « L'ABC de l'expédition » du *Guide des postes du Canada* à ***www.postescanada.ca/guidedespostes***

Le *Guide des postes du Canada* décrit ce que nous acceptons pour les envois du régime intérieur par rapport aux envois du régime international tout en fournissant des renseignements à jour.

Articles à ne pas envoyer

1 Explosifs
- Fusées éclairantes
- Feux d'artifice
- Poudre-éclair
- Grenades
- Propulseurs
- Munitions et cartouches
- Capsules d'armes-jouets et de pistolets de départ
- Fusées-détonateurs et allumeurs

2 Gaz
- Produits en aérosol
- Extincteurs
- Répulsifs à ours et à chiens
- Briquets
- Liquides cryogéniques (azote, hélium, etc.)
- Bouteilles de gaz (oxygène, air, acétylène,propane, butane; dioxyde de carbone, etc.)

3 Liquides inflammables
- Carburant
- Acétone
- Lotion après-rasage
- Parfums
- Adhésifs (colles)
- Peinture, diluants et solvants
- Essence et additifs d'essence
- Alcool (butanol, méthanol, éthanol, etc.)

4 Substances inflammables
- Charbon
- Phosphore
- Coton ou tissus imprégnés d'huile
- Allume-feu, allumettes et tablettes de combustible
- Calcium métal, magnésium métal, sodium métal, etc.

5 Matières oxydantes et peroxydes organiques
- Engrais
- Peroxydes
- Produits chimiques pour piscines
- Trousses de résine époxyde

6 Substances toxiques et infectieuses
- Poisons
- Pesticides
- Produits de préservation du bois
- Bactéries et virus
- Drogues et médicaments
- Produits chimiques pour la photographie
- Sang contaminé et produits biologiques

7 Matières radioactives
- Détecteurs de fumée
- Matières radioactives
- Radio-isotopes à des fins médicales
- Instruments de mesure

8 Matières corrosives
- Colorants
- Acides
- Mercure
- Acide sulfurique
- Produits pour déboucher les tuyaux
- Substances basiques et caustiques (décolorants domestiques, hydroxyde de potassium, hydroxyde d'ammonium, etc.)
- Désinfectants et produits de nettoyage

9 Produits, matières ou organismes divers
- Glace sèche
- Amortisseurs à gaz
- Amiante
- Aimants forts
- Batteries au lithium
- Dispositifs auto gonflables (gilets de sauvetage auto gonflables, coussins pneumatiques, etc.)

Il vous incombe de veiller à ce que votre colis ne contienne aucune marchandise dangereuse. Grâce à votre collaboration, il est possible de prévenir des accidents.
www.postescanada.ca/marchandisesdangereuses

Sans frais : 1 800 267-1177
ATS/ATM : 1 800 267-2797

IS YOUR PACKAGE SAFE TO MAIL?

You could be mailing hazardous materials and not even know it.

Did you know that many common household items are dangerous to ship and are not permitted in the mail?

Even items that are permitted in the mail can present a hazard if improperly packaged, due to vibration, temperature changes and variations in atmospheric pressure.

USPS® is committed to keeping your mail safe. Log on and see if the item you wish to mail is permitted and learn more about how to prepare this type of mail safely.

WARNING: Persons who knowingly mail items or materials that are dangerous or injurious to life, health, or property in violation of 39 USC § 3018 may be liable for a civil penalty of at least $250, but not more than $100,000 for each violation; the costs of any cleanup associated with each violation; and damages.

Visit usps.com/aviationsecurity for more information.

UNITED STATES POSTAL SERVICE

UP IMMEDIATELY

Check for lithium batteries

Electronic equipment containing lithium batteries

If the postal item contains lithium batteries confirm with the sender that the followings conditions are fulfilled:

A. The equipment is acceptable electronic equipment, such as:

Video camera	Walkie-talkie	GPS	Radio-controlled toy
Digital camera	**Scanner**	**Mobile phone**	**MP3 player**
Bluetooth headset	**Smart phone**	**Laptop computer**	**Shaver**
Power drill	**Tablet computer**	**Portable DVD player**	**Measuring equipment**

Note:

a This is a representative listing of common electronic equipment containing four or fewer lithium cells or two or fewer lithium batteries, therefore complying with postal requirements. Acceptance for posting is not exclusive to these items.

b Check that the lithium cells/batteries are installed in the electronic equipment and have not been removed and packaged separately within the outer package.

c Conduct a visual inspection of the outer packaging for damage and check that the packaging used will protect the declared equipment from any damage in the course of operations and air transport.

B. In general, the following equipment is not acceptable since it uses lithium batteries exceeding the watt-hour rating or lithium content, or does not meet the conditions for acceptance by the Post:

Electric bicycle	Laptop with external battery	Electric wheel chair	Small in-house power generator
Battery not installed in handset	160 watt-hour lithium ion loose or installed in equipment	Loose 3.0 watt-hour battery not installed in equipment	Automated external defibrillator (AED)

Note: Lithium batteries packed alone or those packed with equipment are not acceptable in postal items transported by air.

Recognizing Domestic Hazardous Materials

Prohibited

Potentially mailable to domestic destinations*

*Additional requirements in DMM 601.10 and Publication 52 must also be met. Hazard class labels 5.1, 5.2, 8, and 9 must only be used in conjunction with DOT limited quantity markings and only when permitted for the applicable hazard class. For potentially mailable items to international destinations, see the IMM.

The Safety of the Mail is Everyone's Responsibility

Notice 128
September 2012

Your package could not be accepted for one of the following reasons:

- Improper packaging.
- Prohibited or restricted markings and/or labels.
- Stained or leaking mailpiece.

Contact your local Post Office™ to determine if this package is mailable.

Local Post Office telephone and address

Pricing and Classification Service Center

You can get more information from your local Post Office™, your local Business Mail Entry Unit, and the Pricing and Classification Service Center (PCSC), which can be contacted at:

PCSC
90 CHURCH STREET STE 3100
NEW YORK, NY 10007-2951
telephone: 212-330-5300
fax: 212-330-5320

Notice 128
September 2012
PSN 7610-08-000-1489

UNITED STATES POSTAL SERVICE®

What You Can Do to Help

Ask Before You Mail

Many common, everyday items are classified as hazardous materials. Determining the mailability of hazardous materials requires the consideration of a number of factors and can be very challenging. Please check with your local U.S. Postal Service® officials before attempting to mail any items that could be considered hazardous. Improper mailing of hazardous materials may subject you to civil and/or criminal liability.

Full responsibility rests with the mailer to comply with all postal and nonpostal laws and regulations regarding the mailing of hazardous materials.

Mailers are responsible for the following:

- Knowing the physical characteristics of the hazardous materials they wish to mail.
- Ensuring that no hazardous material is mailed unless it is permitted under Postal Service™ mailing standards in *Mailing Standards of the United States Postal Service,* Domestic Mail Manual (DMM®) 601.10 and the *Mailing Standards of the United States Postal Service,* International Mail Manual (IMM®).
- Ensuring that all Postal Service regulations are followed regarding the packaging, markings, labeling, and declaration of hazardous materials placed in the mail.

Further guidance on the packaging, marking, and mailability of hazardous materials is available from the following sources:

- Aviation Mail Security Web site; *http://www.usps.com/ship/can-you-ship-it.htm.*
- DMM 601.10; *http://pe.usps.com/text/dmm300/dmm300_landing.htm.*
- Publication 52, *Hazardous, Restricted, and Perishable Mail; http://pe.usps.com/text/pub52/welcome.htm.*
- IMM (for mailings to foreign addresses); *http://pe.usps.com/text/imm/welcome.htm.*

Reused Packaging

Reused packaging and boxes are only acceptable when all markings and labels are removed or completely marked out so that they cannot be read. Regardless of what is actually inside your package, markings or labels for hazardous or restricted materials may prevent your package from being delivered. Refer to DMM 601.5.1 for more information.

Incorrect Correct

Laws That Keep Us Safe

With certain limited exceptions, the federal law in Title 18 United States Code 1716 (18 U.S.C. 1716) declares it a crime to mail anything that may kill or injure persons or harm property. Persons violating the statute may be subject to fines, imprisonment, or other severe penalties.

The Postal Service has established rules prescribing preparation and packaging conditions under which certain hazardous materials, which are not "outwardly of their own force dangerous or injurious to life, health, or property," may be mailed. Because these rules are very limited, most hazardous materials are prohibited from mailing.

Hazard Classes

For purposes of transportation and shipping, each hazardous material is assigned to a hazard class. The list that follows provides examples of items that are subject to mailing restrictions or prohibitions.

Hazard Classes	Examples
Class 1: Explosives	Fireworks, ammunition, fuses, model rocket engines, automobile air bags
Class 2: Gases	Aerosols, hairspray, scuba tanks, compressed gas containers, lighters, butane, propane
Class 3: Flammable Liquids	Fuels (gasoline), items that contain or used to contain fuel (lighters, propane cylinders, used gasoline tanks), some paints and inks, furniture varnishes, perfumes
Class 4: Flammable Solids	Matches, signal flares
Class 5: Oxidizers and Organic Peroxides	Oxidizing liquids, swimming pool chemicals, peroxides
Class 6: Toxic Materials and Infectious Substances	Insecticides, pesticides, pepper spray, infectious substances, sharps, patient specimens
Class 7: Radioactive Materials	Scientific instruments, products requiring a radioactive warning label
Class 8: Corrosives	Bleach, ammonia, batteries, drain cleaners, mercury, oven cleaners
Class 9: Miscellaneous Hazardous Materials	Magnets, dry ice, self-inflating lifesaving devices, lithium and lithium-ion batteries

Just because an item is NOT on this list does not mean that the item is mailable — be sure to ask before mailing any items that could be considered hazardous.

Check first!

Check that the postal item contains **no dangerous goods** such as those in this list

Examples of dangerous goods prohibited for air transport

1 Explosives

Fireworks
Crackers
Ammunition
Gunpowder
Flares
Warning flares

2 Compressed gases

Butane lighter fuel
Diving tanks
Camping gas
Butane gas
Sprays
Extinguishers

3 Flammable liquids

Oil lighters
Lighter fuels
Oil paints
Adhesion bonds
Flammable perfumes

4 Flammable substances

Matches
Charcoals

5 Oxidizing substances

Oxygen generator chemicals

Peroxides/bleaching powders

6 Toxic and infectious substances

Pesticides
Agricultural chemicals
Mercury compounds
Bacteria
Viruses * Note

7 Radioactive materials

* Note

8 Corrosives

Wet batteries
Mercury
Hydrochloric acid

9 Miscellaneous dangerous goods

Magnetized goods
Engines
Solid carbon dioxide (dry ice)
Lithium batteries * Note

*** Note: Except those that are admissible under the provisions of the UPU Acts.**

A postal item can be accepted only if the description of the contents makes it clear that the item does not contain dangerous goods

Examples of descriptions with which postal items cannot be accepted	Reason why unacceptable	Examples of descriptions with which postal items can be accepted
No description or vague description such as "miscellaneous goods", "daily commodity", or "precision instruments". Product serial numbers instead of descriptions.	Contents are unknown	Wallets, compact discs
Household goods	May contain spray can or compressed gas cylinder	Food, cloth
Sporting goods	May contain aerosol	Racket, ball, shoes
Camping goods	May contain gas cylinder	Tent, sleeping bag
Diving goods	May contain a tank	Wet suit, hydroscope, snorkel
Medical drugs	May contain medical alcohol	Cold medicine, digestive medicine
Cosmetics	May contain flammable perfume, manicure goods, nail-polish remover	Soap, lipstick
Automobile components	May contain flammable fuel additives, aerosols, compressed gas	Mirror, seat cover
Toys	May contain batteries	Toy building blocks

Examples of unacceptable articles

4.1.10. ve 4.1.11 Japonya Posta İdaresi Güvenlik Afişleri

Sayfaya Geri Dön

航空危険物についてのお知らせ

航空危険物が入った郵便物等が、航空機へ積み込まれ、発火するなどした場合、機体を損傷するなどして、重大な事故を引き起こす可能性があり、大変危険です。

安全な運送のため、お引き受けをお断りしたり、また、通常より送達が遅くなる点について、皆様のご理解とご協力をお願いいたします。

その郵便物・荷物ひょっとして 航空危険物ではありませんか？

▶ たとえば、航空危険物にはこのようなものがあります。

火薬類 EXPLOSIVES

花火 Fireworks

クラッカー Crackers

他に、火薬、照明弾、発煙筒、信管、点火コード等

引火性液体 FLAMMABLE LIQUIDS

香水 Perfume

オイルライター Oil Lighter

ライター用燃料 Lighter Fuel

ペイント類 Paint

他に、化学製品、接着剤、アルコール、ガソリン、マニキュア、アロマオイル等

可燃性物質 FLAMMABLE SUBSTANCES

炭 Charcoal

マッチ Matches

酸化性物質類 OXIDIZING SUBSTANCES

小型酸素発生器 Oxygen Generator Chemical

過酸化物 / 漂白剤 Peroxides/Bleaching Powder

他に、ヘアカラー等

毒物類 ※注3 Toxic and Infectious Substances

殺虫剤 Pesticides

農薬 Agricultural Chemicals

他に、水銀化合物、伝染性病原菌、バクテリア、ウィルス、医療系廃棄物、診断用標本等

放射性物質 ※注4 RADIOACTIVE MATERIAL

高圧ガス COMPRESSED GASES

ライター用補充ガス Butane Lighter Fuel

ダイビング用ボンベ Diving Tanks

キャンプ用ガス Camping Gas

カセットコンロ用ガス Butane Gas

スプレー缶 Spray

他に、消火器、酸素ボンベ、ガスライター、ガスシリンダー等

その他の有害物件 ※注1・2 Miscellaneous Dangerous Goods

エンジン Engines

他に、ドライアイス、磁石、シートベルトプリテンショナー、エアバックモジュール、ストーブ等

腐食性物質類 CORROSIVES

液体バッテリー Wet Battery

水銀 Mercury

他に、塩酸等

※注1 この他に、国内については鉄砲、刀剣等の「凶器」も航空危険物として分類されています。
※注2 リチウム電池が組み込まれた電子機器等を郵送する場合は一定の条件を満たすものに限ります。
※注3・4 伝染性物質及び放射性物質については、国際郵便約款の規定に従って差し出されるものを除きます。

▶ 航空危険物が入っていると…

国内あての場合 Domestic Mail △

郵便禁制品（火薬類、ガスボンベ、ガソリン等）以外はお引き受けできますが、航空輸送できないため、配達が遅くなる場合があります。

お客様 → 日本郵便株式会社 → 自動車便、船便又は鉄道コンテナ便 → お届け先

日本郵便株式会社 → 航空機便 ✕ お届け先（送達日数よりも１～４日程度配達が遅れ）

外国あての場合 International Mail ✕

Dangerous Goods Not Permitted to be Transported as International Mail

お引き受けできません！

国際郵便においては、郵便物の種類（通常郵便物、小包郵便物、ＥＭＳ郵便物）及び輸送モード（航空便、ＳＡＬ便、船便）に関わらず、引き受けることができません。

▶ 危険物（郵便物を搭載する航空機等に危険を及ぼす可能性がある爆発物等）がないか、送る前にご確認ください。

お問い合わせ：フリーコール （国内あて）0120-232-886 （外国あて）0120-5931-55

平日8:00～22:00/土・日・休日9:00～22:00

携帯電話から 0570-046-666（通話料有料） For English 0570-046-111

[H25.4.1～H26.3.31]

JP POST 郵便局

Erasing the "dangerous goods label"/ "Marking" indication from the exterior packaging of the mail item

If any of the following "dangerous goods label" / "Marking" is indicated on the exterior of the international mail you are dispatching, we cannot accept it as an international mail item (airmail/ surface mail) as it cannot be determined from the exterior whether dangerous goods are contained or not, even if the articles contained may not fall under the category of dangerous goods.

If the mail item has any of the following indication on its exterior, please erase the indication completely before dispatching the mail item.

List of dangerous goods labels/markings (Example)			
Cannot be sent by international mail ×	Explosives	Flammable gas	Non-flammable, non-toxic gas
	Toxic gas	Flammable liquid	Flammable solid
	Spontaneously combustible	Dangerous When Wet	Oxidizer
	Organic peroxide	Toxic substance	Infectious substance
	Radioactive material (Category No. 1, 2, 3)	Corrosive	Limited quantity of dangerous goods
	Dangerous goods in excepted quantity	Lithium battery handling label	Magnetized material
	Cargo Aircraft Only	Cryogenic Liquid	Keep away from heat
	UN number (UN no.)	UN mark	* Based on the provisions of the Universal Postal Convention, you cannot send by airmail "Dangerous goods by air" as stipulated in the IATA Dangerous Goods Regulations, regardless of airmail (including SAL/EMS) or surface mail (excluding certain exceptions).
	Indication of UN "○○○○"		
Mailing is possible under certain conditions△	Biological substance*	Miscellaneous*	Radioactive material, excepted package
	* Letters containing biological substance (Category B) For mail that contains biological substance (Category B) as stipulated in the terms and conditions of international mail, this label must be indicated on the exterior packaging of the mail item. When dispatching a mail item other than the above, please erase this indication before dispatching the mail item if it is displayed on the exterior of the package.	* Letters containing infectious substances If dry ice is included as coolant of biological substance (Category B) as stipulated in the terms and conditions of international mail, this label must be indicated on the exterior packaging of the mail item. When dispatching a mail item other than the above, please erase this indication before dispatching the mail item if it is displayed on the exterior of the package.	* Letters containing radioactive substance When dispatching letters containing radioactive substances as stipulated in the terms and conditions of international mail, this label must be indicated on the exterior package of the mail item. When dispatching a mail item other than the above, please erase this indication before dispatching the mail item if it is displayed on the exterior of the package.

Examples of mail items which cannot be accepted

Pasted with dangerous goods label (Corrosive) , and with UN mark

Pasted with dangerous goods label (Flammable liquid), and with UN mark

With UN mark

With UN number and UN mark

Pasted with dangerous goods labels (Gas category: Non-flammable, Non-toxic)

With "Dangerous goods in excepted quantity" mark

Pasted with dangerous goods label (Miscellaneous)

Pasted with dangerous goods label (Flammable liquid) , and with UN number/UN mark

How to erase the "Dangerous goods label"/ "Marking"

Examples of exterior packaging which cannot be accepted

Erasing the "Dangerous goods label"/ "Marking"

*When the content is not dangerous goods by air, **please completely erase the hazardous goods label and marking** as follows before dispatching.

4.1.12 ve 4.1.13 Danimarka Posta İdaresi Güvenlik Afişleri

Sayfaya Geri Dön

POST

Forsendelse af Lithium Batterier

Elektronisk udstyr, der indeholder lithium batterier

Hvis forsendelsen indeholder lithium batterier, må den indeholde: Maximum 2 batterier eller 4 celler, der er **installeret** i udstyret.

A. Nedenfor er der eksempler på sådant udstyr ;

Videokamera	Walkie talkies	GPS	Radiostyret legetøj
Digital kamera	**Scanner**	**Mobiltelefon**	**MP3 afspiller**
Bluetooth headset	**Smartphone**	**Bærbar computer**	**Barbermaskine**
Boremaskine	**Tablet**	**Bærbar DVD afspiller**	**Måleinstrument**

Note:

a. Denne oversigt indeholder almindeligt eletronisk udstyr, som indeholder 4 eller færre lithiumceller eller 2 eller færre lithium batterier og derfor kan sendes med post.
b. Lithiumcellerne/batterierne er installeret i det elektroniske udstyr og ikke placeret ved siden af udstyret.
c. Indpakningen skal være fri for skader, og den skal være tilstrækkelig til at kunne tåle normal posthåndtering og transport.

B. Følgende udstyr ikke accepteres, eftersom det skal forsynes med lithium batterier, som ikke opfylder bestemmelserne for at kunne transporteres i postforsendelser.

Elektrisk cykel	Computer med ekstra batteri	Elektrisk rullestol	Elektrisk generator
Batteri som ikke er installeret i headset	160 watt-timers lihitum ion batteri selv om batteriet er installeret i udstyret	Løst 3.0 watt-timers batteri, som ikke er installeret i udstyr	Automatisk extern defibrillator (AED)

Note: Lithiumbatterier, som er pakket ved siden af udstyret, eller forsendelser som alene indeholder lithiumbatterier, kan ikke sendes som postforsendelser.

Juli 2013

Farligt gods!

POST

Eksempel på farligt gods, som er forbudt i postforsendelser:

1. Explosiver

Fyrværkeri
Knaldperler
Ammunition
Krudt
Romerlys
Nødblus

2. Komprimerede gasser

Butangas
Gaslightere
Campinggas
Trykbeholdere
Spraydåser
Brandslukkere

3. Brandfarlige væsker

Benzin
Opløsningsmidler
Maling
Rengøringsmidler
Parfume

4. Brandfarlige faste emner

Tændstikker
Trækul
Stjernekastere

5. Oxiderende emner

Emner, som let antændes af syre
Blegemidler
Hår og textilfarver

6. Giftige og smittefarlige emner

Gifte
Kemikalier
Kviksølvholdige væsker
Bakterier
Virus * Note

7. Radioaktive emner

* Note

8. Ætsende emner

Vådbatterier
Kviksølv
Syrer

9. Øvrige farlige emner

Magnetiske emner
Tøris (dry ice) * Note
Lithium batterier * Note

*** Note: Undtaget, det som er tilladt ifølge bestemmelserne I Post Danmarks Forretningsbetingelser**

Forsendelser kan ikke accepteres hvis det ikke klart fremgår af indholdsbeskrivelsen, at de ikke indeholder farligt gods

Eksempler på beskrivelser, som ikke kan accepteres	Årsag	Eksempel på beskrivelser, som er acceptable
Ingen, eller vag beskrivelse, som f.eks "blandede varer", "dagligvarer", og "Instrument". Produktets serienummer istedet for beskrivelse.	Indholdet er ukendt	Kalender accessories, CD, DVD
Husholdningsartikel	Kan indeholde aerosoldåse eller komprimeret gasflaske	Madvarer, piskeris
Sportsudrustning	Kan indeholde aerosoldåse.	Tennisketscher, bold, sko
Campingudstyr	Kan indeholde gascylinder	Telt, sovepose
Dykkerudstyr	Kan indeholde iltflaske	Våddragt, snorkel
Medicin	Kan indeholde medicinsk alkohol	Forkølelsesmedicin, Mavesårsmedicin
Kosmetik	Kan indeholde parfume, neglelak, Neglelakfjerner	Sæbe, læbestift
Bildele	Kan indeholde benzin, kemiske tilsætningsmidler, aerosoler, komprimeret gas	Spejl, sædeovertræk
Legetøj	Kan indeholde batterier	Legoklodser

Eksempler på ikke acceptable genstande

4.1.14 ve 4.1.15 Kanada Posta İdaresi Güvenlik Afişleri

Sayfaya Geri Dön

POSTES CANADA / CANADA POST

Les symboles courants indiquant la présence de matières dangereuses

COURRIER DU RÉGIME INTÉRIEUR

Si vous trouvez un colis qui porte une étiquette qui est similaire à l'un des exemples illustrés ci-dessous, veuillez aviser votre superviseur.

CES ENVOIS SONT INADMISSIBLES!

Articles qui portent une étiquette similaire à n'importe laquelle des illustrations ci-dessous

CLASS 1
Explosifs

CLASS 2
Gaz comprimés/Gaz

CLASS 3
Liquides inflammables

CLASS 4
Matières solides inflammables dangereuses au contact de l'eau

CLASS 5
Substances comburantes et peroxydes organiques

CLASS 6
Matières toxiques et matières infectieuses

CLASS 7
Matières radioactives

CLASS 8
Matières corrosives

CLASS 9
Matières dangereuses diverses

EXCEPTIONS

Ces envois sont admissibles! Les colis qui sont ornés de ces étiquettes ne peuvent être transportés que par VOIE DE SURFACE. NE PAS LES EXPÉDIER PAR LA POSTE AÉRIENNE.

VOIE DE SURFACE. NE PAS LES EXPÉDIER PAR LA POSTE AÉRIENNE.

90-053-015 (14-02)

CANADA POST
POSTES CANADA
Dangerous Goods Symbols
INTERNATIONAL MAIL
If you encounter a package labelled with a label similar to the examples below, notify your supervisor.
THESE ITEMS ARE NON-MAILABLE!
Items showing a label similar to any of the following depicted below
CLASS 1
Explosives
EXPLOSIVE
1.4
1.5
1.6
CLASS 2
Compressed Gas | Gases
CLASS 3
Flammable Liquids
CLASS 4
Dangerous When Wet
Flammable solids
CLASS 5
Oxidizers and
Organic Peroxides
CLASS 6
Toxic and Infectious
Substances
INFECTIOUS-INFECTIEU
CLASS 7
Radioactive
Substances
CLASS 8
Corrosives
Substances
CLASS 9
Miscellaneous Dangerous Goods
CARGO AIRCRAFT ONLY
FORBIDDEN IN PASSENGER AIRCRAFT
CONSUMER COMMODITY
LIMITED QUANTITY
LTD. QTY.
CAUTION!
LITHIUM BATTERY
DO NOT LOAD OR TRANSPORT PACKAGE IF DAMAGED
MAGNETIZED MATERIAL
CONSUMER COMMODITY
ORM-D
Y
90-053-016 (14-02)

POSTES CANADA POST

Les symboles courants indiquant la présence de matières dangereuses

COURRIER INTERNATIONAL

Si vous trouvez un colis qui porte une étiquette qui est similaire à l'un des exemples illustrés ci-dessous, veuillez aviser votre superviseur.

CES ENVOIS SONT INADMISSIBLES!

Articles qui portent une étiquette similaire à n'importe laquelle des illustrations ci-dessous

CLASS 1
Explosifs

CLASS 2
Gaz comprimés/Gaz

CLASS 3
Liquides inflammables

CLASS 4
Matières solides inflammables dangereuses au contact de l'eau

CLASS 5
Substances comburantes et peroxydes organiques

CLASS 6
Matières toxiques et matières infectieuses

CLASS 7
Matières radioactives

CLASS 8
Matières corrosives

CLASS 9
Matières dangereuses diverses

CONSUMER COMMODITY

LIMITED QUANTITY

LTD. QTY.

CONSUMER COMMODITY
ORM-D

90-053-016 (14-02)

4.1. UPU Güvenlik Dokümanı

Sayfaya Geri Dön

Universal Postal Union

Guidance Materialfor Controlling the Introduction of Dangerous Goods into Postal Networks

Table of contents

		Page
Introduction	4	
1.	Controlling the Introduction of Dangerous Goods into Postal Networks	7
1.1	Dangerous goods training for staff	7
1.2	Reporting and tracking of dangerous goods accidents and incidents to civil aviation authorities and/or other national authorities	8
1.3	Reporting of hidden and undeclared dangerous goods to civil aviation authorities	8
1.4	Methods to inform postal customers of what is admissible in mail at acceptance points	9
1.5	Methods to inform account customers of the restrictions and regulations regarding dangerous goods	9
1.6	Inclusion of clauses in contracts with account customers regarding dangerous goods not permitted in the mail	10
1.7	Emergency procedures	11
1.8	Retentions of documents	11
1.9	Documented acceptance procedures	11
1.10	Procedures of requiring senders information	12
1.11	Procedures for complying with State or Operator variations and changes to the Technical Instructions	
1.12	Procedures for handling rejected packages	12
2. Conclusion		12
3. Attachments		

1. USPS Counter Card–USPS Counter Card.pdf
2. Canada - Dangerous Goods Pamphlet - Canada Post Dangerous Goods Pamphlet.pdf
3. USPS - Acceptance Procedures for Equipment Containing Lithium Batteries - USPS Acceptance Procedures Lithium Batteries.pdf
4. USPS Poster 37 – Is Your Package Safe To Mail? - Poster 37 - Lets Keep the Mail Safe.pdf
5. Check for lithium batteries poster - Check for Lithium Batteries Poster.pptx
6. USPS Notice 128 – Safety of Mail is Everyone's Responsibility - Notice 128 Safety of Mail is Everyone's Responsibility.pdf
7. Dangerous Goods Check First Poster - Dangerous Goods Check First Poster.pptx
8. USPS – Dangerous GoodsWarning Labels Prohibited in International Mail Poster - USPS Dangerous Goods Warning Label Prohibited in International Mail.pdf
9. Dangerous goods prohibited in international mail information sheets - Dangerous goods are prohibited in international postal services.pdf
10. Japan Post - Dangerous Goods Poster - Japan Post DG Poster.pdf
11. Japan Post -Reusing boxes with dangerous goods labels information - Japan Post reused boxes.pdf
12. Denmark – Check for Lithium Batteries - Denmark Check for Lithium Batteries.ppt
13. Denmark – Dangerous Goods Poster - Denmark Dangerous Goods Poster.ppt
14. Canada - Dangerous Goods Symbols Domestic Mail - Canada DG Symbols Domestic.pdf
15. Canada - Dangerous Goods Symbols International Mail - Canada DG Symbols International.pdf

This document is the work of the UPU/PSG – Dangerous Goods Working Group. The information is provided to assist member countries and their designated operators(DO) in protecting their postal networks from the introduction of inadmissible or undeclared dangerous goods into the mail. This is particularly important as it relates to air transport, which is the primary transport mode of international mail.

The International Civil Aviation Organization's (ICAO),Annex 18 The Safe Transport of Dangerous Goods by Air, states as follows:

> **11.4 Dangerous goods by mail**
>
> **Recommendation.** - *Each Contracting State should establish procedures with a view to controlling the introduction of dangerous goods into air transport through its postal services.*
>
> *Note.— International procedures for controlling the introduction of dangerous goods into air transport through the postal services have been established by the Universal Postal Union.*

While ICAO is concerned specifically with the transport of mail by air, these procedures are put in place to protect all modes of transportation, employees, customers, and all others who move mail as part of the global supply chain. The purpose of this manual is to provide guidance to designated operators for putting procedures in place to control dangerous goods, emphasize the new requirements contained in the ICAO Technical Instructions for the Safe Transport of Dangerous Goods by Air, and provide guidance to designated postal operators when meeting with their local civil aviation authorities.

The Posts have a long history of transporting admissible dangerous goods such as admissible patient specimens, admissible infectious substances and admissible radioactive substances. DOs the world over have individual dangerous goods training programs in place. The UPU's Postal Security Group has also worked for more than 15 years to raise awareness about dangerous goods among UPU member countries and has distributed training materials in this regard.

New technologies are emerging continuously, and they sometimes pose risks for air transport. Many recently developed electronic devices, for example, may not be activated during flight because of the dangers that they pose. Flammable substances like aerosols, to take another example, cannot be transported by airmail. Moreover, as new technologies make new products available, the risk posed by the air transport of these products multiplies. As the prices of these products come down and as e-commerce grows, the demand for shipping these products by air grows as well. This demand growth increases the risk of accidents occurring due to the inadvertent non-observation of shipping regulations. The world's Posts taken together constitute a global logistics chain that must work in close collaboration with the aviation sector. The

aviation safety environment today is more complex than before. If aviation safety is to be assured the Posts, too, must conform to the relevant regulations, procedures and training standards observed by other comparable logistics providers.

Given the increasingly complex aviation safety environment and the increased probability of accidents stemming from the inadvertent non-observance of packaging and admissibility regulations across an ever-growing volume of potential dangerous goods, more systematic and structured efforts are called for to reduce the probability of inadvertent introduction of non-permissible dangerous goods into airmail. There is a need to strengthen, adapt and standardize existing dangerous goods training programs and procedures for controlling the introduction of dangerous goods into the mail.

Despite the long relationship posts have with air transport there has traditionally been very little interaction between designated operators and their respective CAAs. DOs over the years have developed individual procedures and training programs to keep dangerous goods out of the mail. Now, however, given the more complex aviation safety environment, it is believed that more formal and structured methodologies to keep dangerous goods out of the mail have become necessary.

Reflecting this need for more formal and structured methodologies, new text in section 2.3 in chapter 2 of the 2013-2014 version of the ICAO Technical Instructions (TIs) states as follows:

"The procedures of designated postal operators for controlling the introduction of dangerous goods in mail into air transport are subject to review and approval by the civil aviation authority of the State where the mail is accepted."

Similarly, section 4.1 in chapter 4 of the same TIs states as that initial and recurrent dangerous goods training programs must be established and maintained by or on behalf of designated postal operators. It further states that dangerous goods training programs must be subject to review and approval by the civil aviation authority of the State where the mail was accepted by the designated postal operator. Having procedures and training programs in place are requirements applicable to all DOs. These requirements in the Technical Instructions are not new – they are effectively a restatement of long-standing text in chapters 10 and 11 of ICAO Annex 18. It is important that DOs and their national CAAs come together to discuss the business model of the posts and to review and update existing procedures for controlling the introduction of dangerous goods and the related training programs.

This material will provide guidance for the Dangerous Goods Training Program that has been developed in collaboration with ICAO, International Air Transport Association (IATA), civil aviation authorities and PSG members. This manual will also serve as guidance material to assist DOs with the assessment by the CAA of their procedures for controlling the introduction of dangerous goods into air transport.

1 Controlling the introductionof dangerousgoods into postal networks

Part 1, Chapter 2, Section 2.3 of the Technical Instructions, Letter Post Regulations Article RL 131, and Parcel Post Regulations Article RC 119 outline those dangerous goods that may be acceptable in international mail for transport by air subject to the provisions of the appropriate national authorities, the technical instructions and UPU Regulations.

All DPOs must have in place procedures for controlling the introduction of dangerous good in the postal system and into air transport. Even if a DPO chooses not to accept those dangerous goods allowed in the mail, they still must have procedures to prevent undeclared or hidden dangerous goods from entering the mail system. The Technical Instructions require the CAA to assess these procedures in cooperation with the DPO.

Doc 9284 Supplement to the Technical Instructions provides guidance material to States for assessing the DPOs procedures for controlling the introduction of dangerous goods. This guide will help DPOs to respond to the their respective CAAs. The following items were outlined in the guidance material as procedures the DPOs should have in place to control the introduction of dangerous goods into air transport.

1.1 Dangerous goods training for staff

As stated earlier the ICAO Technical Instructions now require that dangerous goods training programmes are subject to review and approval by the CAA of the State where the mail is accepted by the designated postal operator. The new instructions also state that staff of designated postal operators must be trained commensurate with their responsibilities. To that the end the UPU has developed a dangerous goods training program that is in line with the content of training courses outlined in table 1-6 of the Technical Instructions.

This training is a baseline program and the DO should meet with their local CAA to discuss the training program. The local CAA may require more or less trainingdepending on national legislation and the DO operational needs.

The DO shallmaintain training records of its employees. The training records must be retained by the employer for a minimum period of thirty-six months from the most recent training completion month and must be made available upon request to the appropriate national authority.There should be a process for refresher training every 24 months or as needed.

The training is titled International Mailing of Dangerous Goods by Air, and the current material can be downloaded from the UPU website.

http://www.upu.int/en/activities/postal-security/dangerous-goods/training-material.html

The training is divided into three separate programs which follow the recommendations in Table 1-6.

A - Dangerous Goods Training for Staff Accepting Mail
B - Dangerous Goods Training for Staff Processing Mail
C - Dangerous Goods Training for Staff Handling, Storing and Loading Mail

Depending on the responsibilities of the employee's position the number of modules differs from category to category.

Examples of possible methods for delivering training include, but are not limited to:

- Classroom training
- Interactive video conferencing
- Web based training
- On line training, local office training, etc.
- Employee meetings for security and safety of mail

1.2 Reporting and tracking of dangerous goods accidents and incidents to civil aviation authorities and/or other national authorities

The UPU issued letter No. 4293(DOT.PSP)1013 dated 11 February 2013, which provided a process for reporting dangerous goods accidents and incidents to the UPU, which would then be shared with ICAO. Your CAA or other national authority may also have a procedure to report these incidents at the national level.

1.3 Reporting of hidden and undeclared dangerous goods to civil aviation authorities

The UPU issued letter No. 4293(DOT.PSP)1013 dated 11 February 2013, which provided a process for reporting discovered hidden and undeclared dangerous goods to the UPU, which would then be shared with ICAO. Your CAA or other national authority may also have a procedure to report the discovery of hidden and undeclared dangerous goods at the national level.

1.4 Methods to inform postal customers of what is admissible in mail at acceptance points (e.g. street post boxes, post offices, agencies, websites)

DOs should have in place measures to inform the public of mailing regulations. This should include information regarding which dangerous goods are acceptable in mail. This information should be available at all locations where mail is deposited (i.e. Post offices, street/collection boxes, contract postal units). This information should be made available to customers even if a DO chooses not to accept dangerous goods. There are several different examples provided as attachments to this document. These examples are taken from other posts and should be adapted to the rules and regulations of your particular post and national laws.

Examples:

- Warning posters about dangerous goods allowed in mail at postal facilities (official and contracted offices)
- Customer briefings by postal representatives
- Warning information to customers on DPO websites
- Other types of notices to customers such as mailed warnings, advertisements, etc.

1.5 Methods to inform account customers of the restrictions and regulations regarding dangerous goods

The DO should be able to show how information regarding dangerous goods in the mail is communicated to customers. This information could be provided through the DO website, direct e-mail, mailed communications, postings in external publications, or personal interactions by DO account representatives.

Examples of possible compliance measures include, but are not limited to:

- Providing informational pamphlets or brochures on dangerous goods to customers on a periodic basis.
- On-going training efforts by the DO to inform each customer of acceptable or prohibited, dangerous goods in the mail.
- Information regarding penalties for account holders who improperly ship dangerous goods.

1.6 Inclusion of clauses in contracts with account customers regarding dangerous goods not permitted in the mail

The DO account representative should provide material to the account customer about what can and cannot be mailed internationally.

The information provided to account customers should reference specific sections of the designated postal operators mailing requirements or regulations. It could also reference other documentation which outlines the specific references to dangerous goods and prohibited items. These documents should be updated regularly by the DO to reflect the current regulations.

Example of contract language:

MAILABILITY AND IMPORTABILITY

All items mailed under this Agreement must conform to the mailability requirements of the designated post operator as detailed in regulations and conform to the importation restrictions of the destination countries. The Mailer is solely responsible for the importation status of the products mailed under this Agreement.

COMPLIANCE

1. The Mailer must comply with all applicable regulations, orders, and demands, and all other applicable laws.

2. All items mailed under this Agreement must conform to the mailability requirements of the DO and conform to the importation requirements of the destination countries. The Mailer is solely responsible for the importation status of the products mailed under this Agreement.

3. The Mailer must provide any necessary documentation, including data provided in electronic format, in connection with each mailing, in the form and at the time specified by the DO, Customs Agencies, local civil aviation authority, a destination country foreign government, or other authority. The Mailer further understands that the failure to provide any such required documentation may result in refusal at acceptance, delay in processing, involuntary seizure by authorities, and/or return of mail to sender.

4. The Mailer must comply with any regulation or order promulgated by the DO, Customs Agencies, civil aviation authorities, a destination country foreign government, or other governmental unit with jurisdiction over mail, to facilitate the Customs processing of its mail, according to any requirements specified by those authorities.

5. This Agreement may be terminated immediately for cause based on the Mailer's failure to comply with all regulations, orders, and demands and all other applicable laws.

Examples of possible compliance measures could include:

- Standard contract language that is included in each business contract.
- Providing informational pamphlets or brochures on dangerous goods to customers on a periodic basis.
- On-going training efforts by the DO to inform each customer of acceptable or prohibited, dangerous goods in the mail.
- Contractual penalty clauses for account holders who improperly ship dangerous goods.

1.7 Emergency procedures

The DO should have in place written standard operating procedures for emergency response to incidents and accidents involving declared and undeclared dangerous goods. These procedures may already be incorporated into existing safety and security procedures. For example a package leaking an unknown substance may be addressed as a hazardous spill.

It is important that security and safety procedures are communicated to the employees. The method may vary and can include formal training, team briefing, verbal and written instructions, leaflets, etc. The level of information/instruction required would depend on the risks that may be encountered at your workplace.

1.8 Retention of documents

The DO should have in place a written policy for the retention of documents relating to dangerous goods. In accordance with the technical instructions any required documentation for the transport of dangerous goods by air at a minimum must be retained for three months after the flight on which the dangerous goods were transported.

1.9 Documented acceptance procedures for staff regarding the dangerous goods allowed by Part 1;2.3 of the Technical Instructions

If a post has chosen to accept any of the dangerous goods admitted exceptionally as described in Letter Post Regulations Article RL 131, Parcel Post Regulations Article RC 119 and in Chapter 2, Section 2.3 of the ICAO Technical Instructionsfor the Safe Transport of Dangerous Goods by Air (Doc 9284), they must have documented acceptance procedures in place. There should be training provided on these acceptance procedures and they should be readily accessible at acceptance locations.

As described in section 1.1, the training will be commensurate with ICAO Annex 18 and the ICAO Technical Instructions for the Safe Transport of Dangerous Goods by Air (Doc 9284), or their National Authority.

1.10 Procedures for requiring the sender's name, address and signature on packages containing dangerous goods

As part of the DOs acceptance procedures the acceptance personnel should be trained to check that names, addresses, andsignatures be legible on all packages. This requirement is also covered in section 1.1, dangerous good training for staff.

1.11 Proceduresfor complying with State or Operator variations and changes to the Technical Instructions

The DO should have in place a procedure or responsible party for ensuring that any State or Operator variations or changes to the Technical Instructions are incorporated and updated into existing procedures.

1.12 Procedures for the handling of packages rejected from transport

The DO should have in place written standard operating procedures for handling packages that are rejected from air transport. These procedures may already be incorporated into existing safety and security procedures. For example a package may contain an item that cannot be transported by air, but it could be transported by other transport modes. The package would be marked for not for transport by air.

It is important that security and safety procedures are communicated to the employees. The method may vary and can include formal training, team briefing, verbal and written instructions, leaflets, etc. The level of information/instruction required would depend on the risks that may be encountered at your workplace.

2 Conclusion

DOs should meet with their respective CAA at the earliest possible opportunity. This will give the DO the opportunity to explain the operations and business model of the post. This information can then be considered by both parties when discussing the way forward for dangerous goods training and procedures for preventing the introduction of dangerous goods into mail and air transport.

It is important to remember that all DOs, irrespective of whether or not they wish to transport equipment containing lithium batteries or other admissible items outlined in Article 16,should have in place procedures for controlling the introduction of dangerous goods into their postal networks in order keep the mail safe and secure.

4.4. ICAO teknik Enstitüsü Personel Eğitim Programı

Sayfaya Geri Dön

Table 1-6. Content of training courses for staff of designated postal operators

≠

Aspects of transport of dangerous goods by air with which they should be familiar, as a minimum	*Designated postal operators*		
	Categories of staff		
	A	B	C
General philosophy	x	x	x
Limitations	x	x	x
General requirements for shippers	x		
Classification	x		
List of dangerous goods	x		
Packing requirements	x		
Labelling and marking	x	x	x
Dangerous goods transport document and other relevant documentation	x	x	
Acceptance of the dangerous goods listed in 1;2.3.2	x		
Recognition of undeclared dangerous goods	x	x	x
Storage and loading procedures			x
Provisions for passengers and crew	x	x	x
Emergency procedures	x	x	x

≠ **CATEGORIES**

A — Staff of designated postal operators involved in accepting mail containing dangerous goods
B — Staff of designated postal operators involved in processing mail (other than dangerous goods)
C — Staff of designated postal operators involved in the handling, storage and loading of mail

Note.— Guidance on the aspects of training to be covered by staff of designated postal operators can be found in S-1;3.

4.4 COMPETENCY-BASED TRAINING AND ASSESSMENT

Competency-based training and assessment should be used in accordance with the general provisions contained in Chapter 2 of the *Procedures for Air Navigation Services — Training* (PANS-TRG, Doc 9868).

Uyuşturucu Madde

Sayfaya Geri Dön

Common Parcel Characteristics

Heavy Tape or Glue
(edges & seams)

Masking Odors (fabric softener)

Masking Odors (motor oil, coffee)

Marijuana

Khat

Amphetamine

Gizleme Metotları

Sayfaya
Geri Dön

Consumer Items

Toys and Children's Items

Chocolate Candy

Heroin hidden underneath a suitcase

Detergent

Full sheet set

Car Parts

UPU Ateşli Silahlar Haritası

Sayfaya Geri Dön

Map showing UPU firearms data

Yasadışı Bahis

Sayfaya Geri Dön

Typical lottery letter and check

Typical victim on Lead List

“Lead lists” with names of victims

$500.00 in your mailbox!!
SECURE AREA
ALLEN CHEATUM
EL PASO, TX
Date 6/3/09
INCLUDE YOUR PHONE NUMBER FOR NOTIFICATION
(915) 593-6944

$500.00 in your mailbox!!
SECURE AREA
GRACE ROBERTSON
HAMMOND, LA
Date 6/1/09
INCLUDE YOUR PHONE NUMBER FOR NOTIFICATION
(985) 345-0152

$500.00 in your mailbox!!
SECURE AREA
MARIE LAPORTE
UPPER DARBY, PA
Date 6/3/09
INCLUDE YOUR PHONE NUMBER FOR NOTIFICATION
(610) 173 9001

$500.00 in your mailbox!!
SECURE AREA
WILLIE STALLION
DETROIT, MI
Date 6/06/09
INCLUDE YOUR PHONE NUMBER FOR NOTIFICATION
(313) 538-1005

$500.00 in your mailbox!!
SECURE AREA
ANN YOUNGDAHL
MUSKEGON, MI
Date 6/3/09
INCLUDE YOUR PHONE NUMBER FOR NOTIFICATION
(231) 733-0764

$500.00 in your mailbox!!
SECURE AREA
VALERIE PIERCE
BYRON CENTER, MI
Date 6/6/09
050119 698694 119172 429929
INCLUDE YOUR PHONE NUMBER FOR NOTIFICATION
(616) 698-6944

$500.00 in your mailbox!!
SECURE AREA
ARMANDO JACOBO
CRP CHRISTI, TX
Date 6/6/09
050119 939899 119172 429929
INCLUDE YOUR PHONE NUMBER FOR NOTIFICATION
(361) 939 8999

SECURE AREA
MARTHA MAYNARD
LANSING, MI
Date 6/1/09
INCLUDE YOUR PHONE NUMBER FOR NOTIFICATION
(517) 482-4590

SECURE AREA
WALTER KIESEL
LIVONIA, MI
Date 6/2/09
INCLUDE YOUR PHONE NUMBER FOR NOTIFICATION
(734) 542-7497

Yasadışı Eczacılık Ürünleri İçeren Posta Kalemleri

Sayfaya
Geri Dön

Identify postal items containing illicit pharmaceuticals

Identify postal items containing illicit pharmaceuticals

Identify postal items containing illicit pharmaceuticals

Identify postal items containing illicit pharmaceuticals

Identify postal items containing illicit pharmaceuticals

Identify postal items containing illicit pharmaceuticals

Identify postal items containing illicit pharmaceuticals