FACILITY SECURITY REQUIREMENTS

TAPA

Transported Asset Protection Association

Transported Asset Protection Association

Tesis Güvenlik Gereksinimleri
FSR 2023

TAPA Standartları

TAPA Americas
5030 Champion Blvd,
G-11 #266 Boca Raton,
Florida 33496
U.S.A.
www.tapaonline.org
Tel. (561) 617-0096

TAPA Asia Pacific
1 Paya Lebar Link, #04-01,
Paya Lebar Quarter,
Singapore 408533

www.tapa-apac.org
Tel. (65) 6514 0892

TAPA EMEA
Pastoor Ohllaan 39
3451 CB Vleuten
The Netherlands

www.tapaemea.org
Tel. +31 19573461

FSR İçindekiler

1. Giriş

1.1 Bu FSR Belgesinin Amacı

Bu Tesis Güvenlik Gereksinimleri (FSR) belgesi, güvenli depolama ve depolama için resmi TAPA Standardıdır. Alıcılar ve Lojistik Hizmet Sağlayıcıları (LSP'ler) ve/veya Sertifikasyon isteyen diğer Başvuru Sahipleri arasındaki iş/güvenlik anlaşmalarında kullanılabilecek ortak bir küresel Standarttır.

Bu Standardın geliştirilmesinde TAPA, depolama hizmetlerinin küresel, bölgesel ve hatta şirketler içinde nasıl sağlandığına ilişkin çoklu farklılıkları ve FSR'nin bir LSP/Başvuru Sahibi tarafından sağlanan hizmetlerin tamamı veya bir kısmı için geçerli olabileceğini kabul eder. Tedarik zincirinin karmaşıklığına ve boyutuna bağlı olarak, TAPA Standartlarına uyum, tek bir LSP/Başvuru Sahibi veya birden fazla LSP/Başvuru Sahibi ve nitelikli alt yükleniciler aracılığıyla sağlanabilir.

Kapsam

TAPA, sertifikasyonu desteklemek için üç seçenek geliştirmiştir:

- Bağımsız Denetim Kuruluşu (IAB) tarafından tek tesis Sertifikasyonu.
- IAB tarafından Çok Tesisli Sertifikasyon.
- LSP/Başvuru Sahibi veya IAB tarafından Yetkili Denetçiler (AA) tarafından Öz Denetim Sertifikası.

Seyirci

TAPA Standartlarının tipik kullanıcıları şunları içerir:

- Alıcı
- LSP'ler/ Başvuru Sahipleri
- Kolluk Kuvvetleri veya diğer devlet kurumları
- Profesyonel Tedarik Zinciri Organizasyonları
- Sigorta

1. Giriş

1.2 TAPA FSR'yi Uygulamak için Kaynaklar

FSR'nin gerekliliklerini karşılayacak kaynaklar, Alıcı ve LSP/Başvuru Sahibi tarafından müzakere edilmedikçe veya başka bir şekilde kararlaştırılmadıkça, LSP'nin/Başvuru Sahibinin sorumluluğunda ve masrafları LSP'nin/Başvuru Sahibinin kendisine ait olacaktır.

1.3 LSP Politikalarını ve Prosedürlerini Koruma

Güvenlik politikaları ve prosedürleri belgelerinin kopyaları, yalnızca LSP/Başvuru Sahibi ve Alıcı arasındaki imzalanmış ifşa sözleşmelerine uygun olarak Alıcıya sunulacak ve gizli bilgi olarak ele alınacaktır.

2. TAPA Hakkında

2.1 TAPA'nın Amacı

Kargo suçları, değerli, yüksek riskli ürün üreticileri ve lojistik hizmet sağlayıcıları için en büyük tedarik zinciri zorluklarından biridir.

Tehdit artık sadece fırsatçı suçlulardan gelmiyor. Bugün, organize suç çeteleri küresel olarak faaliyet gösteriyor ve amaçlarına ulaşmak için araçlara, tesislere ve personele giderek daha karmaşık saldırılar kullanıyor.

TAPA, küresel üreticileri, lojistik sağlayıcıları, yük taşıyıcılarını, kolluk kuvvetlerini ve diğer paydaşları uluslararası tedarik zincirlerinden kaynaklanan kayıpları azaltma ortak amacıyla birleştiren benzersiz bir forumdur. TAPA'nın birincil odak noktası, gerçek zamanlı istihbarat ve en son önleyici tedbirlerin kullanımı yoluyla hırsızlığın önlenmesidir.

2.2 TAPA'nın Misyonu

TAPA'nın misyonu, tedarik zincirinden kaynaklanan kargo kayıplarını en aza indirerek üyelerin varlıklarını korumaya yardımcı olmaktır. TAPA bunu, küresel Güvenlik Standartlarının geliştirilmesi ve uygulanması, tanınmış endüstri uygulamaları, teknoloji, eğitim, kıyaslama, düzenleyici işbirliği ve suç eğilimlerinin ve tedarik zinciri güvenlik tehditlerinin proaktif olarak tanımlanması yoluyla başarır.

3. TAPA Standartları

3.1 TAPA Güvenlik Standartları

Yüksek değerli hırsızlık hedefli kargoların güvenli bir şekilde taşınmasını ve depolanmasını sağlamak için aşağıdaki küresel TAPA Güvenlik Standartları oluşturulmuştur:

- Tesis Güvenlik Gereksinimleri (FSR), özellikle bir tedarik zinciri içinde *güvenli depolama veya transit depolama* için minimum standartları temsil eder .
- Kamyon Taşımacılığı Güvenlik Gereklilikleri (TSR), yalnızca kamyonla taşımaya odaklanır ve özellikle bir tedarik zinciri içinde *ürünlerin karayolu ile taşınması* için minimum standartları temsil eder .

TAPA küresel Güvenlik Standartları, her üç yılda bir gözden geçirilir ve gerektiğinde revize edilir.

Bu belge yalnızca FSR gerekliliklerini ele almaktadır.

- TAPA FSR için sertifikasyon süreci TAPA FSR Sertifikasyon Çerçevesi belgesinde belgelenmiştir.
- TAPA FSR sertifikasyon statüsünü elde etmek için hem TAPA FSR hem de TAPA FSR Sertifikasyon Çerçevesi belgesinin güncel sürümlerine uyulmalıdır.

3.2 Uygulama

TAPA Güvenlik Standartlarının başarılı bir şekilde uygulanması, LSP'lerin (Lojistik Hizmet Sağlayıcıları) / Başvuru Sahipleri, Alıcılar (kargo sahipleri) ve TAPA Yetkili Denetçilerinin birlikte çalışmasına bağlıdır.

4. Yasal Rehberlik

4.1 Kapsam

FSR bir Küresel Standarttır ve resmi feragat süreci yoluyla bir istisna verilmedikçe Standardın tüm bölümleri zorunludur. (Bkz. Bölüm 6.).

4.2 Çeviri

İngilizce'nin ana dil olmadığı ve çevirinin gerekli ve uygulanabilir olduğu coğrafi bölgelerde, FSR'nin herhangi bir çevirisinin veya herhangi bir bölümünün TAPA'nın bu Standartların geliştirilmesi ve yayınlanmasındaki niyetlerini doğru bir şekilde yansıtmasını sağlamak LSP/Başvuru Sahibi ve temsilcilerinin sorumluluğundadır.

4.3 "TAPA" Markası

"TAPA", Taşınan Varlıkları Koruma Derneği'nin tescilli ticari markasıdır ve TAPA'nın resmi olarak tanınan bölgelerinde açık yazılı izni olmadan kullanılamaz. TAPA Standartları ve ilgili materyaller TAPA aracılığıyla ve TAPA tarafından yayınlanır ve TAPA'nın açık yazılı izni olmadan herhangi bir tarafça revize edilemez, düzenlenemez veya değiştirilemez. TAPA markasının kötüye kullanılması, sertifikanın kaldırılmasına veya yasal işlemlere neden olabilir.

4.4 Sorumluluğun Sınırları

TAPA, bu Standartların yayınlanmasıyla, Standartların tam olarak uygulanıp uygulanmadığına bakılmaksızın, tüm kargo hırsızlığı olaylarının önleneceğine dair hiçbir garanti veya güvence vermez. Depodaki kargonun çalınmasından veya FSR Standartları uyarınca depodaki kargonun başka herhangi bir kaybından kaynaklanabilecek herhangi bir sorumluluk, LSP/Başvuru Sahibi ve/veya Alıcının, birbirleriyle yaptıkları sözleşmelerdeki hüküm ve koşullara ve söz konusu yargı alanında geçerli olabilecek herhangi bir yasa veya tüzüğe uygun olarak olacaktır.

5. Sözleşmeler ve Alt Yüklenicilik

5.1 Sözleşmeler

Alıcının varlıklarının güvenli ve emniyetli bir şekilde taşınması, depolanması ve işlenmesi, bir ibraname veya sözleşmede belirtildiği gibi, toplama, nakliye, depolama ve teslimat boyunca LSP/Başvuru Sahibinin, acentelerinin ve taşeronlarının sorumluluğundadır.

FSR'ye atıfta bulunulduğunda veya LSP/Başvuru Sahibi ile Alıcı arasındaki sözleşmeye dahil edildiğinde, LSP'nin/Başvuru Sahibinin güvenlik programında da atıfta bulunulacaktır.

LSP, Alıcıya FSR Sertifikasyonunun kanıtını ve uygun olduğunda FSR gereksinimlerinin karşılandığına dair kanıt sağlayacaktır. Ayrıca, LSP/Başvuru Sahibinin FSR gerekliliklerini yerine getirmediği iddiası, Alıcı ile LSP/Başvuru Sahibi arasında müzakere edilen sözleşmenin şartlarına göre çözülecektir.

5.2 Taşeronluk

Depolama taşeronları, alt yüklenici LSP/Başvuru Sahibinin belirtilen tüm FSR Standartlarını karşılaması için sözleşmeye dayalı bir gereklilik içerir.

5.3 TAPA Şikayet Soruşturması ve Çözümü

TAPA, sertifikalı bir LSP/Başvuru Sahibinin performansıyla ilgili resmi bir şikayet alırsa, TAPA (doğrulamaya tabi olarak), masrafları LSP/Başvuru Sahibine ait olmak üzere yeniden denetim için LSP/Başvuru Sahibi sözleşmesinin yapılmasını isteyebilir. LSP/Başvuru Sahibi denetimde başarısız olursa veya bu sürece uymayı reddederse, sertifikası geri çekilebilir.

6. Feragatler

6. 1 Genel Bakış

Feragat, bir tesisi belirli bir TAPA gerekliliğinden muaf tutmak veya alternatif bir uyumluluk çözümünü kabul etmek için verilen yazılı bir onaydır. Bir LSP/Başvuru Sahibi FSR'deki belirli bir gerekliliği karşılayamıyorsa ve alternatif önlemleri haklı çıkarabiliyorsa, feragat talep edilebilir. Feragatler, belgelendirme süresi boyunca geçerlidir.

Belirli bir güvenlik gereksinimi için tüm feragat talepleri (kısmen veya tamamen), LSP/Başvuru Sahibi tarafından (TAPA web sitesinde bulunacaktır) Bağımsız Denetim Kuruluşuna (IAB)/Yetkili Denetçiye (AA) bir TAPA Feragat Talep formu aracılığıyla sunulmalıdır. Talepte bulunan LSP/Başvuru Sahibi, feragat talebinde sağlanan bilgilerin doğruluğu konusunda tüm sorumluluğu üstlenir.

Her feragat talebi daha sonra IAB/AA aracılığıyla onay için TAPA Bölgesel Feragat Komitesine sunulmalıdır. Talebin eksiksiz olup olmadığına ve TAPA tarafından işlenmesini haklı gösterip göstermediğine karar vermek IAB/AA'nın sorumluluğundadır; Bu, hafifletici faktörlerin ve/veya alternatif güvenlik kontrollerinin doğrulanmasını içerir.

TAPA yetkilileri ve/veya Alıcılar feragat koşullarının değiştiğine itiraz ederse, TAPA resmi bir soruşturmayı tamamlayacak ve LSP/Başvuru Sahibi, feragatin TAPA tarafından iptal edilebileceğini anlayacaktır.

6. 2 Feragat İş Süreci

Bir LSP, FSR'deki belirli bir gereksinimi karşılayamıyorsa, aşağıdaki feragat süreci uygulanır.

Tablo 1: Sorumluluklar: Feragat Başvurusu / Değerlendirmesi

Adım	Sorumluluk	Eylem
1.	LSP/ Başvuru Sahibi	Etki azaltma önlemlerini oluşturur ve doğrular.
2.	LSP/ Başvuru Sahibi	TAPA Feragat Talep formunu doldurur ve IAB/AA'ya gönderir.
3.	IAB/ AA	TAPA Feragat Talep formunda yer alan bilgilerin bütünlüğünü inceler ve doğrular.
4.	IAB/ AA	TAPA Feragat Talep formunu TAPA Bölgesel Feragat Komitesine sunar.
5.	TAPA Bölgesel Feragat Komitesi	İncelemeler, talepte bulunur ve feragatnameyi kabul eder veya reddeder.

6. Feragatler

Feragat Reddedilirse

TAPA Bölgesel Feragat Komitesi feragat talebini onaylamazsa, LSP/Başvuru Sahibinin FSR'nin tüm güvenlik gerekliliklerini uygulaması gerekir.

Feragat Edilirse

TAPA Bölgesel Feragat Komitesi feragat talebini onaylarsa, aşağıdaki eylemler gerçekleştirilecektir:

Tablo 2: Feragat Onayı

Adım	Sorumluluk	Eylem
1.	TAPA Bölgesel Feragat Komitesi	Feragat özelliklerini belgeler ve imzalar.
2.	TAPA Bölgesel Feragat Komitesi	Feragat süresini (en fazla üç yıla kadar) belirtir ve bir kopyasını AA'ya gönderir.
3.	ACAR	LSP'ye/Başvuru Sahibine Feragat Talebinin sonucunu bildirir.
4.	LSP/ Başvuru Sahibi	Feragat gerekliliklerine uygundur. Bunun yapılmaması, feragat onayını geçersiz kılacaktır.

6. 3 Fiziksel Engeller (bölüm 1 kapsamında) ve Yüksek Değerli Kafes için Feragatler (HVC, bölüm 4.5 kapsamında)

TAPA, aşağıdaki ön koşulların tümünün karşılanması durumunda çevre bariyeri gereksinimlerinin tamamından veya bir kısmından ve/veya HVC'den feragat etmeyi değerlendirecektir:

Genel:

- Feragat talebi, resmi TAPA Feragat Talep formu süreci kullanılarak gönderilir ve IAB/AA tarafından onaylanır.
- Feragat talebi, savunmasız malların gereksiz hırsızlık veya kayıp riski altında olmamasını sağlamak için hafifletici önlemlerin ayrıntılarını içerir.
- Bir risk değerlendirmesi tamamlanmalı ve feragat talebiyle birlikte sunulmalıdır. Risk değerlendirmesinde tespit edilen önemli güvenlik açıkları, feragatnamede ayrı olarak listelenmeli ve riski kabul edilebilir bir düzeye indirmek için alınan önlemler alınmalıdır.

6. Feragatler

Muafiyet talebinin sunulmasında yürürlükte olması ve belgelenmesi gereken hafifletme önlemleri:

- **Çevre bariyerleri:**
  - Yetkisiz kişilerin veya araçların zamanında tespit edilmesine yardımcı olmak için getirilen ek ekipman, kaynaklar ve prosedürler, ek aydınlatma, CCTV kapsama alanı, gelişmiş kişiler ve araç kimliği uygulama prosedürleri, LSP yeleği veya yalnızca tek tip kısıtlı alanları içerebilir ancak bunlarla sınırlı değildir.
  - "İzinsiz erişim yok", "İzinsiz park edilemez" yazan yerel dilde görünür çevre işaretleri yerleştirilmelidir.
  - Dış rıhtım kapılarına veya duvarlara, sürücülere, ziyaretçilere vb. uygun lobiye, güvenlik kontrolüne geçmeleri talimatını veren görünür işaretler yerleştirilecektir.
  - Kargo elleçleme, sevkiyat ve teslim alma alanlarının en az haftada bir denetlenmesini ve feragat koşullarına uygun olmasını sağlayan prosedürlerin yürürlükte olduğunun teyidi.

- **HVC:**
  - HVC feragatleri için, riski en aza indirmek için uygun azaltma eylemleri (bir HVC'nin mevcut olmadığı durumlarda) yıllık Risk Değerlendirmesinde dikkate alınmalı ve belgelenmelidir.
  - Feragat talebi, LSP/Başvuru Sahibi tarafından imzalanan ve hiçbir Alıcının HVC'ye ihtiyaç duymadığını şart koşan ekli bir beyanı içerir.

7. Tesis Güvenlik Gereksinimleri

Bölüm	Genel gereksinimler:	A	B	C
7.0				
7.0.1	Bu Standardın gerektirdiği tüm prosedürler veya politikalar belgelendirilmelidir.	✔	✔	✔
7.0.2	Yönetim, TAPA FSR, SCARS kapatma, risk değerlendirmesi, yönetim raporu ve şirket tedarik zinciri güvenlik gerekliliklerinin sürdürülmesinden sorumlu olan yerinde güvenlik için resmi olarak bir kişi (AA) atamış olmalıdır. FSR programının izlenmesinden başka bir kişi (aynı olabilir) de sorumlu olacaktır. Bu, uyumluluk kontrollerinin planlanmasını, AA'larla iletişimi, yeniden sertifikalandırmayı, FSR Standardındaki değişiklikleri vb. içerir. *Not: Bu kişiler, bu rolü yerine getirmek için sözleşmeli bir çalışan veya dış kaynaklı kişi olabilir.*	✔	✔	✔
7.0.3	Güvenlik yönetim sistemi ile ilgili iç denetimler (işlevler arası bir ekip tarafından), dahili AA tarafından yapılan öz değerlendirme raporları ve SCARS kapanışı tamamlanmalı ve belgelenmelidir.	✔	✔	✔
7.0.4	Fiziksel ve elektronik anahtarları yöneten ve kontrol eden fiziksel kilitler, erişim kartları ve/veya anahtarlar için bir prosedür, kayıt ve/veya anahtar planı gereklidir. Prosedür, çoğaltma, depolama ve eksik/kayıp anahtarlara yanıt verme işlemlerini içermelidir.	✔	✔	✔
7.0.5	Güvenlikle ilgili olayların olasılığını ve etkisini tanıyan bir risk değerlendirmesi en az yılda bir kez yapılmalı ve güncellenmelidir. Yönetim, belirlenen risklerin değerlendirildiğini ve riskleri kabul edilebilir bir seviyeye indirmek veya ortadan kaldırmak için uygun kontrollerin uygulandığını kabul etmelidir. En azından, aşağıdaki yaygın iç/dış olaylar değerlendirilmelidir: kargo veya bilgi hırsızlığı, tesislere veya kargoya yetkisiz erişim, güvenlik sistemlerinin kurcalanması/imha edilmesi, kargonun hayali olarak teslim alınması, işgücü kıtlığı veya doğal afetler sırasında güvenlik sürekliliği, zemin seviyesinden erişilebilir pencereler veya rıhtım kapıları için anti-ram bariyerlerine duyulan ihtiyaç vb. Yerel/ülke risklerine bağlı olarak ek olaylar düşünülebilir.	✔	✔	✔
7.0.6	Başvuru sahibi / LSP (LSP AA olarak adlandırılır) için iç veya yıllık denetimler yapan kişi eğitilmelidir. Bu kişi, 7.0.2'te belirtilenle aynı kişi olabilir veya bu rolü yerine getirmek için sözleşmeli olarak dış kaynaklı bir kişi olabilir.	✔	✔	✔
7.0.7	FSR'yi anlamak ve tüm gerekliliklerini yerine getirebilmek için, tüm başvuru sahibi/LSP AA'larının, denetlemeleri gereken TAPA Standardı ve sürümü için geçerli sınava girmiş ve geçmiş olması gerekir.	✔	✔	✔

Bölüm	Çevre	A	B	C
7.1				
Depo Dış Kargo Elleçleme, Sevkiyat ve Kabul Sahası (Genel)				
7.1.1	CCTV (Kapalı Devre Televizyon) / VSS (Video Gözetim Sistemi) harici kargo elleçleme, nakliye ve teslim alma sahasındaki (giriş ve çıkış noktaları dahil) tüm trafiği görüntüleyerek, operasyonel ihtiyaçlar nedeniyle geçici bir engel olmadıkça tüm araçların ve bireylerin her zaman tanınabilir olmasını sağlar (yani, gerçek zamanlı olarak kamyon yükleme ve boşaltma).	✔	✔	
7.1.2	Yükleme ve boşaltma alanlarında yeterli aydınlatma. *Not: Aydınlatma sabit olabilir, alarm, hareket, ses algılama vb. ile etkinleştirilebilir ve anında aydınlatma sağlanabilir.*	✔	✔	✔
7.1.3	Yetkisiz araçların ve kişilerin harici kargo elleçleme, sevkiyat ve teslim alma sahasında nasıl yönetileceğini açıklayan prosedür. Prosedürle ilgili talimat, gardiyanlar da dahil olmak üzere ilgili iş gücü üyelerine iletilmelidir.	✔	✔	✔
7.1.4	Kargo elleçleme, sevkiyat ve teslim alma sahası, yetkisiz erişimi önlemek için yeterince kontrol edilir.		✔	✔
7.1.5	Zemin seviyesinden erişilebilir pencereler veya rıhtım kapıları için, yıllık Risk Değerlendirmesi, anti-ram bariyerlerine olan ihtiyacı değerlendirmelidir. Ek olarak, iç mekanların yetkisiz olarak görüntülenmesini önlemek için pencere kapaklarının kullanımının değerlendirilmesini içermelidir (Bkz. Risk Değerlendirmesi, Bölüm 7.0.5.).	✔		
Fiziksel Engeller				
7.1.6	Fiziksel bariyer, kargo elleçleme, nakliye ve kabul sahasını kapsar.	✔		
7.1.7	Kargo elleçleme, nakliye ve kabul sahası etrafındaki fiziksel bariyer minimum 6 fit / 1.8 metre yüksekliğe sahiptir. *Not: Yetkisiz erişimi önlemek için tasarlanmış fiziksel bariyer, zemin seviyesinin değiştiği, yani daha düşük olduğu alanlar da dahil olmak üzere tüm uzunluğu boyunca 6 fit/1.8 metre yüksekliğinde olmalıdır.*	✔		
7.1.8	Kargo elleçleme, nakliye ve kabul sahası etrafındaki fiziksel bariyer iyi durumda tutulmuştur.	✔		
7.1.9	Kargo elleçleme, sevkiyat ve alım sahası bariyerleri içindeki kapı(lar) insanlı veya elektronik olarak kontrol edilir.	✔		
7.1.10	Kargo elleçleme, sevkiyat ve teslim alma sahası etrafındaki fiziksel bariyer, en az haftada bir bütünlük ve hasar açısından denetlenir.	✔		
Dış Rıhtım Alanları				
7.1.11	Renkli veya "gündüz/gece" dış CCTV/VSS kameralarla kaplı harici Dock alanları.	✔	✔	✔
7.1.12	CCTV / VSS Kameralar, operasyonel ihtiyaçlardan kaynaklanan geçici bir engel olmadıkça (yani gerçek zamanlı olarak kamyon yükleme ve boşaltma) dış rıhtım alanı etrafındaki tüm işlemleri ve hareketleri her zaman görüntüleyebilmek için monte edilmiştir.	✔	✔	✔

Bölüm	Çevre	A	B	C
7.1.13	Dış rıhtım alanlarının etrafındaki tüm araçlar ve bireyler CCTV / VSS kameralarla kapsanmalıdır. araç kimlik bilgilerini net bir şekilde gösterebilen ve personelin yüz özelliklerini ayırt edebilen. *Not: TAPA, kamera çözünürlüğüne yükseltme yeteneği olmayan mevcut sertifika sahiplerinin 2026 revizyonuna kadar mevcut çözünürlükleriyle devam etmelerine izin verecektir. Yeni sertifika sahipleri veya yeni siteler yeni gereksinimi karşılamalıdır.*	✔		
7.1.14	Dış rıhtım alanlarının etrafındaki araçlar ve bireyler, çoğu durumda CCTV/VSS kameraları tarafından örtülmeli ve görülebilmelidir.		✔	✔
7.1.15	Rıhtım kapılarının etrafındaki tüm dış alanlar tamamen aydınlatıldı.	✔	✔	✔
Kişisel Araç Erişimi				
7.1.16	Kişisel araçlar, yalnızca önceden onaylanmışsa ve işaretli/belirlenmiş park alanlarıyla sınırlıysa kargo elleçleme, sevkiyat ve teslim alma alanlarına izin verilir. Dış rıhtım alanlarına 25 m yürüme mesafesinde kişisel park yeri yoktur. Ön onay ve kısıtlamalar için süreçler yürürlüktedir.	✔	✔	✔

Bölüm	Dış Duvarlar, Çatı ve Kapılar	A	B	C
7.2				
Tesisin Dış Tarafları: CCTV				
7.2.1	Tesisin tüm dış taraflarını kaplayan renkli veya "gündüz/gece" dış CCTV/VSS kamera.	✔		
7.2.2	Tesisin dış taraflarını kapılar, pencereler veya diğer açıklıklarla kaplayan renkli veya "gündüz/gece" dış CCTV/VSS kamera sistemi.		✔	
7.2.3	Dış CCTV / VSS kamera sisteminin tüm görünümleri, operasyonel ihtiyaçlar nedeniyle geçici bir engel olmadıkça (yani gerçek zamanlı olarak kamyon yükleme ve boşaltma) her zaman açıktır.	✔		
7.2.4	Tesislerin dış taraflarındaki tüm araçlar ve bireyler, araç kimlik bilgilerini açıkça gösterebilen ve personelin yüz özelliklerini ayırt edebilen CCTV / VSS kameraları ile kapsanmaktadır.	✔		
7.2.5	Çoğu durumda dış CCTV / VSS kameraları tarafından görülebilen araçlar ve bireyler.		✔	
Dış Duvarlar ve Çatı				
7.2.6	Dış duvarlar ve çatı, penetrasyona dayanacak şekilde tasarlanmış ve bakımı yapılmıştır (Örnek: tuğla, blok, yukarı eğimli beton döşeme, sandviç panel duvarlar).	✔	✔	✔
7.2.7	Tesis dış duvarlarındaki herhangi bir açılabilir pencere, havalandırma deliği veya diğer açıklıklar veya tesis dış duvarlarındaki çalışma zemininden 3 metreden daha aşağıya monte edilen herhangi bir sızdırmaz pencere, fiziksel bir bariyere sahip olmalı veya alarma geçirilmeli ve ana alarm sistemine bağlanmalıdır.	✔	✔	
7.2.8	Tesis çatısındaki herhangi bir açılabilir pencere, tavan penceresi, havalandırma, erişim kapağı veya diğer açıklıklar fiziksel bir bariyere sahip olmalı **veya** alarma geçirilmeli ve ana alarm sistemine bağlanmalıdır.	✔		

Bölüm	Dış Duvarlar, Çatı ve Kapılar	A	B	C
7.2.9	Çatıya dış erişim (merdiven veya merdivenler) şu şekilde olmalıdır: Fiziksel olarak kilitlenir ve CCTV/VSS (Renkli veya "gündüz/gece" kameralar) ile kaplıdır. veya Fiziksel olarak kilitlendi ve alarma geçti.	✔		
7.2.10	Çatıya (merdiven veya merdiven) dışarıdan erişim fiziksel olarak kilitlenir.		✔	✔
7.2.11	Tüm tesis harici depo kapıları ve ofis kapıları, yetkisiz açılmayı algılamak için alarma geçirilir ve ana alarm sistemine bağlanır. *Not: Yükleme kapıları bu gereklilik kapsamında değildir, yükleme kapısı alarm gereksinimleri için bölüm 7.2.17'ye bakın.*	✔	✔	✔
7.2.12	Her tesis harici depo kapısı, ofis kapısı veya diğer açıklıklar, ana alarm sistemi içindeki kapı veya bölge başına benzersiz bir şekilde tanımlanmalıdır.	✔		
7.2.13	Tüm harici depo kapıları, aktif kullanımda değilken her zaman kapalı ve emniyete alınmıştır. Uygun olduğunda, Anahtarlar / Kodlar Kontrol Edilir.	✔	✔	
7.2.14	Depo yaya kapıları ve çerçeveleri kolayca delinemez. Dışarıda menteşeler varsa, sabitlenmeli veya punta kaynağı yapılmalıdır. Cam kırılma dedektörleri takılmadıkça veya başka bir yerel algılama cihazı kapak sağlamadıkça (örneğin PIR) ve doğrudan izleme merkezine alarm verilmedikçe veya cam çubuklar/ağ ile korunmadıkça cam kapılar kabul edilemez.	✔	✔	✔
7.2.15	Sadece acil durum amaçlı kullanılan acil çıkışlar (Örn: Yangın çıkışları), her zaman bireysel veya bölgeli sesli bir siren ile alarma geçirilir.	✔	✔	
7.2.16	Tüm rıhtım kapıları, küçük portatif el aletleri kullanılarak zorla girişi caydıracak ve/veya geciktirecek şekilde yeterli güçtedir.	✔	✔	✔
7.2.17	**Rıhtım Kapıları** **Çalışma dışı saatler:** Rıhtım kapıları kapalı, güvenli (yani elektronik olarak devre dışı bırakılmış veya fiziksel olarak kilitli). Yetkisiz izinsiz girişleri tespit etmek ve ana alarm sistemine bağlı bir alarm oluşturmak için alarm verilen yükleme kapıları. **Çalışma saatleri:** Yükleme kapıları aktif kullanımda değilken kapalı olmalıdır. Makaslı kapılar, kullanılıyorsa, mekanik sürgü/mandal kilidi ile sabitlenmeli ve en az 8 fit/2.4 metre yüksekliğinde olmalıdır.	✔	✔	✔

Bölüm	Ofis ve Depo Giriş ve Çıkış Noktaları	A	B	C
7.3				
Ofis Alanı Ziyaretçi Giriş Noktası/Noktaları				
7.3.1	Ziyaretçi giriş noktası/noktaları, yaka kartı verilmesi, kontroller, kayıt kaydı, ziyaretçiler, refakatçi gereksinimi vb. konularda eğitim almış bir çalışan/bekçi/resepsiyon görevlisi tarafından kontrol edilir (çalışma saatleri dışındaki ziyaretler için geçerli olan süreç).	✔	✔	✔
7.3.2	CCTV ile kapsanan ofis alanı ziyaretçi giriş nokta(lar)ı; (Renkli veya "gündüz/gece" kameralar) bireyler her zaman açıkça tanınabilir.	✔	✔	
7.3.3	Zorlama alarmı ofis alanı ziyaretçi giriş noktalarında bulunur ve haftalık olarak test edilir.	✔	✔	
7.3.4	Ofis alanına gelen tüm ziyaretçiler, devlet tarafından verilmiş fotoğraflı kimlik (örn. ehliyet, pasaport veya nüfus cüzdanı vb.) kullanılarak tanımlanır.	✔	✔	✔
7.3.5	Ofis alanına gelen tüm ziyaretçiler en az 30 gün boyunca kayıt altına alınır ve kayıt tutulur.	✔	✔	✔
7.3.6	Ziyaretçi tesisten ayrılırken tüm ziyaretçi yaka kartları mutabakata kavuşturulmalı ve günlük olarak tam kayıt kontrol edilmelidir.	✔	✔	
7.3.7	Tüm ziyaretçiler görünür bir şekilde yaka kartları veya geçiş kartları gösterir ve şirket personeli tarafından eşlik edilir.	✔	✔	
İş Gücü Giriş Noktaları				
7.3.8	İş gücü giriş noktaları, erişim 7/24 kontrol edilir.		✔	✔
7.3.9	7/24 elektronik erişim kontrol cihazı ile kontrol edilen işgücü giriş noktaları. Erişim günlüğe kaydedildi.	✔		
7.3.10	CCTV kapsamındaki işgücü giriş noktaları. (Renkli veya "gündüz/gece" kameralar).	✔	✔	
7.3.11	İncelemeden sonra, tüm çalışanlara şirket fotoğraflı kimlik kartları verilmelidir.	✔	✔	
7.3.12	Diğer tüm çalışanlara, tesis içinde tanınmalarını sağlamak için bir şirket kimlik kartı sağlanmalıdır.	✔	✔	
7.3.13	Tüm çalışanların rozetleri açıkça gösterildi.	✔	✔	
7.3.14	İş Gücü Rozetleri hiçbir koşulda paylaşılmamalı ve rozet düzenleme politikası uygulanmalıdır.	✔	✔	
Sürücü ve Araç Tanımlama				
7.3.15	Devlet tarafından verilmiş fotoğraflı kimlik (örn. ehliyet, pasaport veya nüfus cüzdanı vb.) kullanılarak tanımlanan tüm sürücüler ve bir sürücü kaydı tutulur.	✔	✔	✔
7.3.16	Sürücü belgesinin geçerli olduğunun, sürücü fotoğraflı kimliğinin süresinin dolmadığının ve sürücüyle eşleştiğinin doğrulanması.	✔	✔	✔
7.3.17	Araç tanımlayıcıları manuel olarak (yani yazılı) veya kameralarla kaydedilir. Minimum plaka ve araç tipini ekleyin.	✔		

Bölüm	Depo ve Ofis İçi	A	B	C
7.4				
Depo Alanı: Çok Kiracılı Duvarlar				
7.4.1	İç zeminden tavana çok kiracılı duvarlar ve çatı, penetrasyona direnecek şekilde inşa edilmiş/tasarlanmış ve bakımı yapılmıştır (Örnek: tuğla, blok, yukarı eğimli beton döşeme, sandviç panel duvarlar).	✔	✔	✔
7.4.2	İç zeminden tavana çok kiracılı duvarlar güvenlik sınıfı tel örgüden veya endüstri tarafından tanınan diğer güvenli bariyerlerden yapılmışsa, izinsiz girişleri tespit etmek için de alarm verilmelidir. *Not: Ağ, düşük dereceli eskrim veya güvenlik sınıfı olmayan ağ kabul edilemez.*	✔	✔	✔
İç Depo Alanları				
7.4.3	İzinsiz giriş algılama (örn. kızılötesi, hareket, ses veya titreşim algılama), dahili depo alanlarını izlemek için gereklidir. Alarmlar, çalışma dışı saatlerde (yani depo kapalıyken) etkinleştirilmeli ve ana alarm sistemine bağlanmalıdır. *Not: Depo gerçek bir 7/24/366 operasyonsa, riskler ve azaltıcı etkenler yerel Risk Değerlendirmesinde belgelenmişse bu gereklilik Yok olabilir . (Bkz. Bölüm 7.0.5)* *Çalışma saatlerinden bağımsız olarak, ofis ve depodaki dış kapılarda ve zemin kat pencerelerinde her zaman çevre izinsiz giriş tespiti veya fiziksel bariyerler gereklidir. (Bkz. bölüm 7.2.11).*	✔		
İç Rıhtım Kapıları ve Rıhtım Alanları				
7.4.4	Tüm iç rıhtım kapıları ve rıhtım alanları CCTV ile kaplıdır. (Renkli veya "gündüz/gece" kameralar).	✔	✔	✔
7.4.5	Tüm iç rıhtım kapılarında ve rıhtım alanlarında yüklenen/boşaltılan yükün görünümleri, operasyonel ihtiyaçlar nedeniyle geçici bir engel olmadıkça (yani gerçek zamanlı olarak kamyon yükleme ve boşaltma) her zaman açıktır.	✔	✔	✔
7.4.6	Kargo hareketi veya hazırlama alanlarında %100 CCTV gözetimi altındaki alıcı varlıkları (örn. palet kırılması/birikme alanları, depolama raflarına giden ve gelen yollar, rıhtım, transit koridorları).	✔	✔	
Ofis ve rıhtım/depo arasında erişim kontrolü				
7.4.7	Ofis ve rıhtım/depo arasında erişim kontrollü.	✔	✔	
7.4.8	Ofis ile rıhtım/depo arasındaki kapılar için kartlı erişim veya interkom kapı alarmları yerel olarak duyulabilir **ve** 60 saniyeden fazla açık tutulduğunda veya zorla açıldığında hemen yanıt için bir alarm üretir.	✔		
7.4.9	Ofis ve rıhtım/depo arasındaki kapılar için kapı alarmları yerel olarak duyulabilir **veya 60 saniyeden fazla açık tutulduğunda** veya zorla açıldığında yanıt için alarm gönderir.		✔	
7.4.10	LSP'lerin/Başvuru Sahibinin yetkili işgücünün ve refakatçi ziyaretçilerin, bir iş ihtiyacına göre rıhtım/depo alanlarına erişimine izin verildi ve kısıtlandı.	✔	✔	✔
7.4.11	Erişim izninin yalnızca belirlenmiş/yetkili personele verildiğini sınırlamak/doğrulamak için en az üç ayda bir gözden geçirilen rıhtım/depo alanlarına erişim listesi.	✔	✔	
Yüksek Değerli Kafes (HVC) / Alan				

Bölüm	Depo ve Ofis İçi	A	B	C
7.4.12	HVC'nin boyutu ve kullanımı, Alıcı/LSP/Başvuru Sahibi sözleşmesi ile belirlenebilir. Bir anlaşma yoksa, HVC en az 6 metreküp ürün depolayabilmelidir.	✔	✔	
7.4.13	HVC / Alan çevresi, üst / çatı dahil olmak üzere her tarafta kafesli veya sert duvarlı.	✔	✔	
7.4.14	Kapıda/kapıda HVC/ Alan kilitleme cihazı.	✔	✔	
7.4.15	HVC girişinde ve iç alanda eksiksiz CCTV/VSS (Renkli veya "gündüz/gece" kameralar) kapsama alanı. *Not: HVC, içeride bir kamera bulamayacak kadar küçükse, girişin kamera kapsama alanı yeterlidir.*	✔		
7.4.16	HVC girişinde CCTV (Renkli veya "gündüz/gece" kameralar) kapsama alanı.		✔	
7.4.17	HVC'ye 10'dan fazla kişinin erişmesi gerekiyorsa, erişim kart/anahtarlık ile elektronik olarak kontrol edilmelidir. 10 veya daha az kişi tarafından erişim gerekiyorsa, kontrollü bir anahtar verme sistemi tarafından desteklenen ağır hizmet tipi kilit veya asma kilit sistemi. Anahtarlar, bir vardiyayı kapsayacak şekilde kişilere imzalanabilir, ancak onay alınmadan aktarılmamalı ve anahtar günlüğüne kaydedilmelidir. Kullanılmadığında iade edilecek ve hesaba katılacak tüm anahtarlar.	✔		
7.4.18	HVC kapıları/kapıları, zorla girişi algılamak için alarm verir. Alarmlar, yetkisiz erişimi tespit etmek için kapı kontakları ve/veya CCTV/VSS hareket algılama kullanılarak oluşturulabilir.	✔		
7.4.19	HVC'nin çevresi iyi durumda tutulur ve bütünlük ve hasar açısından aylık olarak denetlenir.	✔		
7.4.20	HVC'ye erişimin yalnızca atanmış/yetkili personele verilmesini sağlamak için LSP/ Başvuru Sahibi. HVC'ye onaylanan erişim listesi aylık olarak gözden geçirilir ve çalışan işten ayrıldığında veya artık erişim gerektirmediğinde gerçek zamanlı olarak güncellenir. HVC erişimi için prosedür uygulandı.	✔	✔	
Depodan Çöp Kontrolü				
7.4.21	İç ve/veya dış depo ana çöp toplama kutuları/sıkıştırma alanları CCTV/VSS ile izlenmektedir.	✔		
7.4.22	Depo içinde kullanılan çöp torbaları kullanıldığı yerlerde şeffaftır.		✔	✔

Ön Yükleme ve Evreleme				
7.4.23	Alıcı ve LSP/Başvuru Sahibi arasında karşılıklı olarak mutabık kalınmadıkça, FTL/özel Alıcının kamyonlarının çalışma saatleri dışında depo tesisinin dışına önceden yüklenmesi veya park edilmesi yasaktır. Alternatif güvenlik önlemleri uygulanmalıdır (örneğin, konteyner üzerinde ek güvenlik cihazları). *Not: "Depo tesisinin dışında", tesisten ayrı, uzakta, ancak yine de LSP'nin/Başvuru Sahibinin bahçesinin/çevre çitinin içindeki alanlardır.*	✔	✔	✔
Kişisel Konteynerler ve Çıkış Aramaları				
7.4.24	Yazılı güvenlik prosedürleri, 'kişisel konteynerlerin' depo içinde nasıl kontrol edildiğini tanımlar. Kişisel kaplar arasında öğle yemeği kutuları, sırt çantaları, soğutucular, cüzdanlar vb. bulunur.	✔	✔	
7.4.25	Yerel yasalar izin veriyorsa, LSP/Başvuru Sahibi, çıkış aramaları için belgelenmiş bir prosedür geliştirmeli ve sürdürmelidir. Prosedürün etkinleştirilmesi, LSP/Başvuru Sahibinin takdirine ve/veya Alıcı/LSP/Başvuru Sahibi sözleşmesine göredir. Prosedür, en azından, normalde gerekli olmadığında (örneğin, işgücü hırsızlığından şüphelenildiğinde) arama yapma ihtiyacı ortaya çıkması durumunda, LSP'nin/Başvuru Sahibinin arama hakkı kriterlerini ele almalıdır.	✔		
Kargo Elleçleme Ekipmanlarının Kontrolü				
7.4.26	Tüm forklift ve diğer elektrikli kargo elleçleme ekipmanlarının çalışma saatleri dışında devre dışı bırakılmasını gerektiren prosedür. *Not: Buna el krikoları/transpaletler dahil değildir.*	✔	✔	
konteyner veya treyler bütünlüğü; 7 nokta denetimi				
7.4.27	Tüm giden özel Alıcı konteynerlerinde veya römorklarında gerçekleştirilen 7 noktalı fiziksel muayene: Ön Duvar, Sol Taraf, Sağ Taraf, Zemin, Tavan/Çatı, İç/Dış Kapılar ve Kilitleme Mekanizması, Dış/Alt Takım. *Not: Bu, kilitli ve/veya mühürlü her türlü treyler ve konteyner için geçerlidir (örn. Deniz taşımacılığı konteynırları ile sınırlı değildir).*	✔	✔	✔
Yük Devir Teslim Süreci; Güvenlik Mühürleri				
7.4.28	Alıcı tarafından özel olarak muaf tutulmadıkça, tüm doğrudan, kesintisiz gönderilerde kurcalanmaya karşı korumalı güvenlik mühürleri kullanılır. Contalar ISO 17712'ye (I, S veya H sınıflandırması) göre sertifikalandırılacaktır. *Not: Birden fazla mühür taşıyan sürücülerle ilişkili karmaşıklık ve risk nedeniyle, birden fazla duraklı gönderilerde mühür gerekli değildir.*	✔	✔	✔
7.4.29	LSP/Başvuru Sahibi, güvenlik mühürlerinin, treyler (konteyner) kapı kilitlerinin, pim kilitlerinin ve diğer güvenlik ekipmanlarının yönetimi ve kontrolü için belgelenmiş prosedürlere sahip olmalıdır .	✔	✔	✔
7.4.30	Güvenlik mühürleri, yalnızca güvenliği ihlal edilmiş mühürleri tanıması ve bildirmesi talimatı verilen yetkili personel, yani depo personeli tarafından yapıştırılır veya çıkarılır. Mühürler, Alıcı muafiyeti olmadıkça sürücü tarafından asla yapıştırılmamalı veya çıkarılmamalıdır.	✔	✔	✔

7.4.31	Güvenliği ihlal edilmiş güvenlik mühürlerini tanımak ve raporlamak için yürürlükte olan prosedürler.	✔	✔	✔
Kargo Bütünlüğü; Yükleme/Boşaltma Doğrulama Süreci				
7.4.32	Gönderilen ve alınan tüm Alıcı varlıklarının, manuel ve/veya elektronik parça sayımı yapılarak devir teslim noktasında doğrulanmasını sağlayan sağlam prosedürler. Süreç, anormalliklerin tutarlı bir şekilde tanınmasını, belgelenmesini ve LSP/Başvuru Sahibi ve/veya Alıcıya bildirilmesini sağlamalıdır. Manuel ve/veya elektronik kayıtlar kanıt niteliğinde olmalıdır. Sürücüler bu faaliyete tanık olmak için hazır bulunmuyorsa, Alıcı/LSP/Başvuru Sahibi, taramalar ve/veya CCTV/VSS görüntüleri gibi alternatif sayım doğrulamasının bu amaç için özel olarak toplanmasını ve saklanmasını sağlamalıdır. *Not: Eksik parçalara ek olarak, anormallikler arasında olası bir hırsızlık veya hırsızlığa işaret eden hasar, eksik kayışlar veya bantlar, kesikler veya diğer belirgin açıklıklar yer alabilir.*	✔	✔	✔
Hileli Teslim Almalar				
7.4.33	Kamyon sürücüsü kimliği, kargo teslim alma belgeleri ve Alıcı tarafından belirtilen geçerli ön uyarı ayrıntıları, yüklemeden önce doğrulanır. Prosedür yerinde olmalıdır.	✔	✔	✔

Bölüm	**Güvenlik Sistemleri; Tasarım, İzleme ve Yanıtlar.**	**A**	**B**	**C**
7.5				
İzleme Gönderisi				
7.5.1	Alarm olaylarının dahili veya 3. taraf harici bir izleme direği aracılığıyla 366 gün 7 gün 24 saat izlenmesi, yetkisiz erişime karşı korunması. *Not: İzleme gönderileri site içinde veya dışında bulunabilir ve şirkete ait veya üçüncü taraf olabilir. Her durumda, erişim bir elektronik erişim kontrol sistemi (rozetler), kilitler veya biyometrik tarayıcılar kullanılarak kontrol edilmelidir.*	✔	✔	✔
7.5.2	Tüm güvenlik sistemi alarmlarına gerçek zamanlı olarak 7x24x366 yanıt vermek için izleme direği.	✔	✔	✔
7.5.3	İzleme direği, alarm aktivasyonunu onaylar ve 3 dakikadan daha kısa sürede yükselir.	✔	✔	✔
7.5.4	Alarm izleme raporları mevcuttur.	✔	✔	✔
7.5.5	Yanıt sonrası prosedürleri yerinde izleyin.	✔	✔	✔
İzinsiz Giriş Tespit Sistemi (IDS)				
7.5.6	Tüm IDS, çalışma saatleri dışında etkinleştirilir ve ana alarm sistemine bağlanır.	✔	✔	✔
7.5.7	60 günlük IDS alarm kayıtları tutulur.	✔	✔	
7.5.8	IDS alarm kayıtları güvenli bir şekilde saklanır ve yedeklenir.	✔		
7.5.9	IDS alarm kayıtları güvenli bir şekilde saklanır.		✔	

Bölüm	Güvenlik Sistemleri; Tasarım, İzleme ve Yanıtlar.	A	B	C
7.5.10	IDS erişiminin yetkili kişiler veya sistem yöneticileriyle sınırlı olmasını sağlama prosedürü. Buna sunucular, konsollar, denetleyiciler, paneller, ağlar ve veriler dahildir. Erişim ayrıcalıkları, kişiler kuruluştan ayrıldığında veya artık erişim gerektirmeyen rolleri değiştirdiğinde derhal güncellenmelidir.	✔	✔	✔
7.5.11	IDS'nin elektrik kesintisi / kaybı durumunda iletilen alarm. *Not: Kesintisiz Güç Kaynağı (UPS) olan sistemler için, UPS aküsü arızalandığında alarm iletilir.*	✔	✔	✔
7.5.12	IDS alarmı, doğrulamayı yerinde ayarladı. *Not: Alarmların çalışma dışı saatlerde devreye girdiğini doğrulayan prosedürler.*	✔	✔	✔
7.5.13	Sabit hat veya kablosuz ve/veya iletişim modu arızası yoluyla iletilen IDS alarmı.	✔	✔	
7.5.14	IDS cihazında ve/veya hat arızasında yedek iletişim sistemi.	✔	✔	
Otomatik Geçiş Kontrol Sistemi (AACS)				
7.5.15	90 günlük AACS işlem kayıtları mevcuttur. Kayıtlar güvenli bir şekilde saklanır; Yedekle.	✔	✔	
7.5.16	AACS erişiminin yetkili kişiler veya sistem yöneticileriyle sınırlı olmasını sağlama prosedürü. Erişim ayrıcalıkları, kişiler kuruluştan ayrıldığında veya artık erişim gerektirmeyen rolleri değiştirdiğinde derhal güncellenmelidir.	✔	✔	
7.5.17	Düzensizlikleri veya kötüye kullanımı (yani birden fazla başarısız deneme, yanlış okumalar (yani devre dışı bırakılmış kart), yetkisiz erişime izin vermek için kart paylaşımı kanıtı vb.) belirlemek için en az üç ayda bir gözden geçirilen erişim sistemi raporları. Süreç yerinde.	✔	✔	
Kapalı devre televizyon				
7.5.18	CCTV/VSS'nin dijital kaydı yerinde.	✔	✔	✔
7.5.19	CCTV/VSS için kayıt hızı, kamera başına minimum 8 kare/saniye (fps) olarak ayarlanmıştır.	✔	✔	✔
7.5.20	Dijital kayıt işlevi, prosedür aracılığıyla operasyonel günlerde günlük olarak kontrol edilir. Kayıtlar mevcut.	✔	✔	✔
7.5.21	CCTV/VSS kayıtları, yerel yasaların izin verdiği durumlarda en az 30 gün süreyle saklanır. LSP/Başvuru Sahibi, CCTV kullanımını yasaklayan ve/veya video veri depolamasını 30 günden daha kısa bir süre ile sınırlayan yerel yasaların kanıtını sağlamalıdır.	✔	✔	✔
7.5.22	Donanım, yazılım ve veri/video depolama dahil olmak üzere CCTV/VSS sistemine sıkı bir şekilde kontrol edilen erişim. CCTV/VSS depolama sistemi, erişim kontrolleri yerinde olan tesis içindeyse bu oda kilitlenmelidir.	✔	✔	✔

Bölüm	Güvenlik Sistemleri; Tasarım, İzleme ve Yanıtlar.	A	B	C
7.5.23	CCTV/VSS görüntüleri, güvenlik amacıyla, sadece yetkili personel tarafından izlenir.	✔	✔	✔
7.5.24	Yerel yasalara uygun olarak gerçek zamanlı ve arşiv görüntülerinin kullanımına ilişkin CCTV/VSS veri koruma politikasını detaylandıran prosedürler.	✔	✔	
Dış ve İç Aydınlatma				
7.5.25	Dış ve iç aydınlatma seviyeleri, inceleme ve kanıt kalitesinde görüntü kaydına izin veren CCTV görüntülerini desteklemek için yeterlidir.	✔	✔	
7.5.26	Dış ve iç aydınlatma seviyeleri, tüm araçları ve bireyleri net bir şekilde tanımak için yeterlidir.	✔		

Bölüm	Eğitim ve Prosedürler	A	B	C
7.6				
Eskalasyon Prosedürleri				
7.6.1	Alıcının kayıp, kayıp veya çalıntı varlıklarının zamanında bildirilmesi süreci de dahil olmak üzere, Alıcının varlıklarının ele alınması için yürürlükte olan yerel prosedürler. LSP/Başvuru Sahibi tarafından 24 saat içinde Alıcıya bildirilecek olaylar. Bariz hırsızlıklar hemen bildirildi. Süreç sürekli olarak takip edildi.	✔	✔	✔
7.6.2	Listelenen ve mevcut güvenlik olayları için Acil Durum Alıcısı ve LSP/ Başvuru Sahibi tesis yönetimi irtibat kişileri. Liste her 6 ayda bir güncellenir ve kolluk kuvvetlerinin acil durum irtibat kişilerini içerir	✔	✔	✔
Yönetim Taahhüdü				
7.6.3	Yönetim, tüm ilgili kişilerin (yani çalışanlar ve yükleniciler) sağlayıcının güvenlik beklentilerinin açıkça farkında olmasını sağlamak için bir güvenlik politikası geliştirmeli, iletmeli ve sürdürmelidir.	✔	✔	✔
Antrenman				
7.6.4	İşe girişin ilk 60 günü ve sonrasında her 2 yılda bir iş gücünün tüm üyelerine verilecek Güvenlik/Tehdit Farkındalığı eğitimi.	✔	✔	✔
7.6.5	Bilgi güvenliği farkındalığı eğitimi, Alıcının bilgilerine erişimi olan işgücüne sağlanan Alıcının elektronik ve fiziksel gönderi verilerini korumaya odaklanmıştır.	✔	✔	✔
Alıcının Varlıklarına Erişim				
7.6.6	Alıcının varlıklarını (yani kargoyu) işgücünün, ziyaretçilerin vb. yetkisiz erişimine karşı korumak için yürürlükte olan prosedür(ler).	✔	✔	
Bilgi Kontrolü				
7.6.7	Nakliye belgelerine ve Alıcının varlıklarına ilişkin bilgilere erişim, "bilmesi gerekenlere" göre kontrol edilir.	✔	✔	✔
7.6.8	Nakliye belgelerine ve Alıcının varlıklarına ilişkin bilgilere erişim, izlenir ve kaydedilir.	✔	✔	✔
7.6.9	Nakliye Belgeleri ve Alıcının varlıklarına ilişkin bilgiler, imha edilene kadar korunur.	✔	✔	✔
Güvenlik Olayı Raporlama				

Bölüm	Eğitim ve Prosedürler	A	B	C
7.6.10	Proaktif önlemleri uygulamak için kullanılan güvenlik olayı raporlama ve izleme sistemi.	✔	✔	
Bakım Programları				
7.6.11	Her zaman işlevselliği sağlamak için tüm teknik (fiziksel) güvenlik kurulumları/sistemleri için yürürlükte olan bakım programları (örn. CCTV/VSS, Erişim Kontrolleri, İzinsiz Giriş Algılama ve Aydınlatma).	✔	✔	✔
7.6.12	Önleyici bakım yılda bir kez veya üreticinin spesifikasyonlarına uygun olarak yapılır.	✔	✔	✔
7.6.13	Tüm sistemlerin işlevsellik doğrulamaları haftada bir kez ve sistem arızası anında/otomatik olarak bildirilmedikçe veya alarm verilmedikçe belgelenir.	✔	✔	
7.6.14	Arızanın tespit edilmesinden sonraki 48 saat içinde bir onarım emri başlatılmalıdır. 24 saati aşması beklenen onarımlar için alternatif azaltıcı etkenler uygulanmalıdır.	✔	✔	
Yüklenici Oryantasyonu				
7.6.15	LSP/Başvuru Sahibi, tüm alt yüklenicilerin/satıcıların LSP/Başvuru Sahibi ile ilgili güvenlik programlarından haberdar olmasını ve bunlara uymasını sağlamak için.	✔	✔	✔
Sevkiyat ve Teslim Alma Kayıtları				
7.6.16	Gönderi ve Teslim Alma Belgeleri okunaklı, eksiksiz ve doğru (yani saat, tarih, imzalar, sürücü, nakliye ve teslim alma personeli, gönderi detayları ve miktarı vb.).	✔	✔	✔
7.6.17	LSP / Başvuru Sahibi, iki yıldan az olmayan bir süre boyunca tüm tahsilatların ve teslimat kanıtlarının kayıtlarını tutmalı ve gerektiğinde bunları zarar soruşturmalarına sunmalıdır.	✔	✔	✔
7.6.18	Teslimat kanıtı, Alıcı ile LSP/Başvuru Sahibi arasındaki yazılı anlaşmaya uygun olarak, Alıcının talep ettiği durumlarda, varış yerinin, gönderinin alınmasından itibaren kararlaştırılan zaman dilimi içinde menşei bilgilendirmesi ve uyarı öncesi gönderi ayrıntılarını uzlaştırması sağlanmalıdır.	✔	✔	✔
Ön uyarı süreci yürürlükte				
7.6.19	Alıcının talep ettiği durumlarda, gelen ve/veya giden gönderilere uygulanan ön uyarı süreci yürürlüktedir. Ön uyarı ayrıntıları, Alıcı ve LSP/Başvuru Sahibi tarafından kararlaştırılmalıdır. Önerilen ayrıntılar şunları içerir: kalkış saati, tahmini varış saati, kamyon şirketi, sürücü adı, plaka ayrıntıları, gönderi bilgileri (parça sayısı, ağırlık, konşimento numarası vb.) ve römork mühür numaraları.	✔	✔	✔

Bölüm	İş Gücü Bütünlüğü	A	B	C
7.7				
7.1	**Tarama/İnceleme/Geçmiş Kontrolleri (yerel yasaların izin verdiği şekilde)**			
7.7.1	LSP/Başvuru Sahibi, en azından geçmiş istihdam ve sabıka geçmişi kontrollerini içeren bir tarama/inceleme/arka plan sürecine sahip olmalıdır. Tarama/inceleme, çalışanlar ve yükleniciler de dahil olmak üzere tüm başvuru sahipleri için geçerlidir. LSP/Başvuru Sahibi, TAS işçilerini tedarik eden müteahhitlik şirketlerinde de eşdeğer bir sürecin uygulanmasını talep edecektir.	✔	✔	✔

Bölüm	İş Gücü Bütünlüğü	A	B	C
7.7.2	TAS çalışanının, mevcut bir sabıkası olmadığına ve LSP'nin/Başvuru Sahibinin güvenlik prosedürlerine uyacağına dair beyanname imzalaması gerekmektedir.	✔	✔	✔
7.7.3	LSP/Başvuru Sahibi, TAS çalışanlarını sağlayan ajans ve/veya taşeron tarafından sağlanan gerekli tarama/inceleme/arka plan bilgilerine sahip olmak için anlaşmalara sahip olacak veya bu taramayı kendileri yapacaktır. Tarama, sabıka geçmişi kontrolü ve istihdam kontrollerini içermelidir.	✔	✔	✔
7.7.4	Başvuranın / işgücünün işe alım öncesi ve sonrası yanlış beyanı ile başa çıkma prosedürü.	✔	✔	✔
İşgücünün Feshi veya Yeniden İşe Alınması *Not: Fesih, hem gönüllü hem de gönülsüz ayrılmaları içerir - işten çıkarılan ve istifa eden iş gücü üyeleri.*				
7.7.5	Şirket kimliklerini, erişim rozetlerini, anahtarları, ekipmanları, BT varlıklarını ve hassas bilgileri dahil etmek için sonlandırılan iş gücünden fiziksel varlıkları kurtarın. Belgelenmiş prosedür gerekli.	✔	✔	✔
7.7.6	Alıcının verilerini koruyun: İşten çıkarılan işgücünün, Alıcının verilerini (envanter veya programlar) içerenler de dahil olmak üzere fiziksel veya elektronik sistemlere erişimini sonlandırın Prosedür gereklidir.	✔	✔	✔
7.7.7	Doğrulama için işe alım ve işe alım için iş gücü kontrol listesi.	✔	✔	✔
7.7.8	Yeniden işe alma: Reddetme/fesih kriterleri hala geçerliyse, LSP/Başvuru Sahibinin işgücünü yeniden işe almasını önlemek için prosedürler mevcuttur. *Not: Kayıtlar yeniden işe alınmadan önce gözden geçirilir (Ör: daha önce işten çıkarılan personelin geçmişi veya – reddedilen başvuru sahipleri (daha önce istihdamı reddedilen).*	✔	✔	✔

8. Merkezi İşlev Gereksinimleri (Yalnızca Çoklu site sertifikasyonu için geçerlidir)

Bölüm	Merkezi İşlev	A	B	C
8.1	**Genel**			
8.1.1	Çoklu tesis sertifikasyonu kapsamında tanımlandığı gibi tüm tesisler için güvenlik yönetim sistemini yönetmek için merkezi bir işlev vardır.	✔	✔	✔
8.1.2	Tüm siteler, merkezi işlevle yasal veya sözleşmeye dayalı bir ilişkiye sahip olacaktır.	✔	✔	✔
8.1.3	Sistem içindeki tüm tesislerinin geçerli TAPA Güvenlik Standardının gereksinimlerini karşıladığından emin olmak için tek bir güvenlik yönetim sistemi kurulmuştur.	✔	✔	✔
8.1.4	Merkezi fonksiyon ve yönetim sistemi, TAPA Standartlarına sürekli uyumu sağlamak için iç denetimlere tabi tutulacaktır.	✔	✔	✔

Bölüm	Merkezi İşlev	A	B	C
8.1.5	Merkezi işlev, her bir tesisin geçerli TAPA FSR gerekliliklerini karşıladığından emin olmak için kapsam dahilindeki sahaların denetimlerini gerçekleştirecektir. Denetimler uygun TAPA denetim şablonlarıyla yapılmalıdır. Tüm bireysel yıllık saha denetimleri tamamlanmalı ve belgelendirme sürecinden önce denetçiye sunulmalıdır.	✔	✔	✔
8.1.6	Merkezi işlev, tüm tesislerin TAPA Güvenlik Standartlarına uymasını zorunlu kılma ve gerektiğinde düzeltici ve önleyici eylemleri uygulama yetki ve haklarına sahip olacaktır. *Not: Uygulanabilir olduğunda bu, merkezi işlev ile siteler arasındaki resmi anlaşmada belirtilmelidir.*	✔	✔	✔
8.2	**8.2 Politikalar ve Prosedürler**			
8.2.1	Merkezi işlev, tüm tesisleri için geçerli olan güvenlik yönetim sistemleri için belgelenmiş politika ve prosedürleri sürdürecektir.	✔	✔	✔
8.2.2	Merkezi işlev, uygun politika ve prosedürlerin gerektiğinde tüm siteler tarafından güncellenmesini, iletilmesini, dağıtılmasını ve uygulanmasını sağlayacaktır.	✔	✔	✔
8.2.3	Politikalar ve prosedürler korunacak ve gerektiğinde tüm siteler tarafından kolayca erişilebilir olacaktır.	✔	✔	✔
8.3	**8.3 Tüm tesisler için gerçekleştirilen Öz Değerlendirme denetim raporu**			
8.3.1	Merkezi işlev, tüm tesislerin öz değerlendirme yapmasını zorunlu kılar ve tüm öz değerlendirme raporları, kayıtlar ve incelemeler için merkezi birime sunulur. Kayıtlar en az iki (2) yıl süreyle saklanmalıdır.	✔	✔	✔
8.3.2	Merkezi işlev, güvenlik yönetim sistemlerini iyileştirmek için öz değerlendirme ve denetimlerden kaynaklanan tüm SCAR'ların uygun şekilde kapatılmasını sağlayacaktır.	✔	✔	✔
8.3.3	Tüm siteler, bekleyen tüm SCAR'larla ilgili ilerleme güncellemelerini ve raporları merkezi işleve gönderecektir. SCAR'ların vade tarihlerinden önce tamamlanmaması durumunda, merkezi işlev LSP'lerin/Başvuru Sahibinin yönetimine iletilecektir. Kayıtlar en az iki (2) yıl süreyle saklanmalıdır.	✔	✔	✔
8.4	**8.4 Denetim kayıtları, günlükler (ziyaretçi kayıtları, Sürücü kaydı,), 7 noktalı denetimler**			
8.4.1	Merkezi işlev, tüm tesislerin teftiş kayıtlarını, ziyaretçi kayıtlarını, sürücü kayıtlarını ve 7 noktalı teftiş vb. kayıtlarını tutmasını sağlamak için prosedürlere sahip olacaktır.	✔	✔	✔
8.5	**8.5 Tüm sitelerin Risk Değerlendirmeleri**			
8.5.1	Merkezi fonksiyon, tüm sahalarda uygun risk değerlendirmelerinin ve yönetiminin yapılmasını ve kayıtlarının en az iki (2) yıl süreyle tutulmasını sağlamak için prosedürlere sahip olacaktır.	✔	✔	✔
8.6	**Sitelerin CCTV ve alarm düzeni**			
8.6.1	Merkezi işlev, tüm tesislerin CCTV ve alarm düzeni gibi tüm fiziksel güvenlik sistemlerindeki belgeleri gözden geçirmesini ve korumasını sağlayan prosedürlere sahip olacaktır.	✔	✔	✔
8.7	**Alarm ve Erişim Kontrolü kayıtları**			
8.7.1	Merkezi işlev, tüm Alarm ve Erişim Kontrol sistemlerinin operasyonel etkinliklerini sağlamak için bakımının yapılmasını ve test edilmesini sağlayan prosedürlere sahip olacaktır.	✔	✔	✔

Bölüm	Merkezi İşlev	A	B	C
8.7.2	Merkezi işlev, tüm sitelerin tüm izinsiz giriş tespiti ve erişim kontrolü testlerinin ve olaylarının kayıtlarını tutmasını sağlayan prosedürlere sahip olacaktır.	✔	✔	✔
8.8	**Eğitim kayıtları**			
8.8.1	Merkezi işlev, tüm tesislerin çalışanlarının güvenlik yönetimi eğitimi hakkında uygun eğitim kayıtlarını tutmasını sağlamak için prosedürlere sahip olacaktır.	✔	✔	✔
8.8.2	Merkezi işlev, tüm tesislerin tüm site personelinin güvenlik eğitimi kayıtlarını tutmasını sağlamak için prosedürlere sahip olacaktır. Kayıtlar en az iki (2) yıl süreyle saklanmalıdır.	✔	✔	✔
8.9	**8.9 Tarama/inceleme kayıtları**			
8.9.1	Merkezi işlev, güvenlik yönetim sistemlerinin bütünlüğünü ve etkinliğini sağlamak için tüm tesislerin düzenli aralıklarla kayıtların taranmasını ve incelenmesini gerçekleştirmesini sağlayacak prosedürlere sahip olacaktır.	✔	✔	✔
8.9.2	Merkezi işlev, bulguları ve düzeltici/önleyici 8.1.6 eylemleri de dahil olmak üzere gözden geçirme kayıtlarının tutulmasını sağlamak için prosedürlere sahip olacaktır. Kayıtlar en az iki (2) yıl süreyle saklanacaktır.	✔	✔	✔
8.10	**8.10 Öz denetimleri değerlendirmek için Yönetimin Gözden Geçirmesi; SCAR'lar yükseltildi; herhangi bir kayıp, hırsızlık; Risk Değerlendirmeleri.**			
8.10.1	Merkezi fonksiyon, güvenlik yönetim sistemlerine uyumu, etkinliği ve iyileştirmeyi sağlamak için asgari olarak düzenli yönetim incelemesi yapacaktır.	✔	✔	✔
8.10.2	Yönetim incelemeleri, diğerlerinin yanı sıra, öz denetimlerin etkinliğini, SCAR'ların kapatılmasını, risk değerlendirmelerini, olayları ve iyileştirme eylemlerini kapsayacaktır.	✔	✔	✔
8.10.3	Merkezi işlev, tüm yönetim incelemelerinin kayıtlarını en az iki (2) yıl süreyle tutacaktır.	✔	✔	✔

9.0. BT ve Siber Güvenlik Tehdidi – Gelişmiş Seçenek

FSR, daha yüksek bir koruma seviyesi olarak kabul edilen ve modüllere ek olarak kullanılabilen isteğe bağlı Siber Güvenlik Tehdidi geliştirmelerini içerir. Bu isteğe bağlı geliştirmenin, LSP/Başvuru Sahibi ve/veya Alıcısı tarafından operasyonel güvenlik ihtiyaçları için ek gereksinimler olarak seçilmesi amaçlanmıştır. Bu isteğe bağlı geliştirme, sertifikasyon öncesi değerlendirmede sertifikasyon denetiminin bir parçası olarak seçildiğinde, tüm gereksinimler zorunlu hale gelir.

Bölüm	BT ve Siber Güvenlik Tehdidi – Gelişmiş Seçenek
9.	**Zorunlu gereklilikler**

Bölüm	BT ve Siber Güvenlik Tehdidi – Gelişmiş Seçenek
9.1	LSP/Başvuru Sahibi, BT ve siber tehdit için güvenlik politikalarına sahip olmalıdır. İlkeler ayrı veya birleştirilmiş bir belgede olabilir. Politikalar şunları açıklamalıdır: - 1. LSP'nin/Başvuru Sahibinin tehditleri belirleme ve bunlara yanıt verme eylemleri. 2. Güvenlik olaylarını korumak, algılamak, test etmek ve yanıtlamak için yürürlükte olan ilkeler ve yordamlar. 3. BT sistemlerinin ve/veya verilerinin kurtarılması için yöntemler. 4. Olayın öğrenilmesinden sonraki 24 saat içinde tedarik zinciri etkisini azaltmak için Alıcılara/Müşterilere iletişim protokolü. 5. Politikaların yıllık olarak nasıl gözden geçirildiği ve uygun şekilde nasıl güncellendiği.
9.2	LSP/Başvuru Sahibi, tüm çalışanlara bilgi farkındalığı eğitimi vermelidir. Bu eğitim: - 1. Bilgisayar kullanıcılarının güvenliği ve ilgili faydaları sağlamadaki rollerini ve sorumluluklarını kapsar. 2. Eğitim alan kişilerin kayıtlarının en az 2 yıl süreyle tutulmasını ve saklanmasını sağlayan bir sisteme sahip olun.
9.3	LSP/Başvuru Sahibi, aşağıdakileri sağlayan alt yükleniciler ve/veya satıcılarla Siber Güvenlik önlemlerinin alınmasını sağlamak için yazılı bir politikaya sahip olmalıdır: 1. LSP'lerin/Başvuru Sahibinin Siber Güvenlik gereksinimleri alt yüklenicilere ve/veya satıcılara iletilir ve sözleşmelere dahil edilir. 2. Alt yüklenicilerin ve/veya satıcıların LSP'nin/Başvuru Sahibinin Siber Güvenlik gereksinimlerini tanımadığı veya benimsemeyi reddettiği durumlarda, LSP'nin/Başvuru Sahibinin Siber Güvenlik gereksinimlerine ve müşterilerine yönelik riskleri azaltan önlemler belgelenir ve uygulanır.
9.4	LSP/Başvuru Sahibi, gücün en az 48 saat boyunca kritik BT sistemlerine (yerel risk değerlendirmesinde tanımlanan) yönlendirilmesini sağlayan bir Güç Kesintisi Azaltma planına (örneğin alternatif güç kaynağı veya yedek jeneratör) sahip olmalıdır.
9.5	LSP'lerin/Başvuru Sahibinin Bilgi Sistemlerinde lisanslı anti-virüs ve kötü amaçlı yazılımdan koruma yazılımı yüklü olmalıdır. Virüsten koruma ve kötü amaçlı yazılımdan koruma yazılımı en son güncellemeleri içermelidir.
9.6	LSP/ Başvuru Sahibi, gerekli tüm veri ve yazılım yedekleme ve kurtarma düzenlemeleri dahil ancak bunlarla sınırlı olmamak üzere, güvenliği ihlal edilmiş sistem saldırılarından kurtulmak için uygun BT Felaket Kurtarma Planına (DRP) sahip olmalıdır.
9.7	LSP'lerin/Başvuru Sahibinin Bilgi Sistemleri yedeklenmelidir. Bu tür yedeklemeler düzenli olarak test edilmeli ve yedekleme verileri şifrelenmeli ve ikincil, site dışı bir konuma aktarılmalıdır.
9.8	LSP/Başvuru Sahibi, benzersiz bireysel tanımlayıcılar ve güçlü parolalar kullanarak Bilgi Sistemlerine erişimi yönetmek ve kontrol etmek için tüm kullanıcı hesapları için bir politika uygulamalıdır. Aşağıdakileri sağlamak için yürürlükte olan prosedürler: 1. Parola uyumluluğu denetim programı uygulandı. 2. Oluşturma sırasında her yeni hesaba benzersiz bir başlangıç parolası atanmalıdır. 3. İlk parolalar kullanıcının adını, kimlik numarasını içeremez veya kullanıcı bilgilerine dayalı standart bir kalıbı izleyemez. 4. Parolalar kullanıcılara güvenli bir şekilde ve yalnızca kullanıcının kimliği doğrulandıktan sonra iletilecektir. 5. Kullanıcıların ilk oturum açma sırasında parolalarını değiştirmeleri gerekir. 6. Parolalar en az 90 günde bir değiştirilmelidir.

Bilginize: Stanvdardın sağlanan ulusal dile tercümesi, TAPA 2023 gerekliliklerinin anlaşılmasına yardımcı olmayı amaçlamaktadır. Standardın çevirisi, bilgimiz dahilinde ve gerekli arka plan bilgisiyle başlatıldı ve doğrulandı. Ancak ilgili standardın orijinal İngilizce versiyonu denetimle alakalıdır ve öyle kalacaktır.

Yayınlanma geçmişi

İlk olarak Ağustos 2023'te yayınlandı

Ağustos 2023'te yayınlanan ilk (Mevcut) baskı

Bu Kamuya Açık Şartname 15 Eylül 2023'te yürürlüğe girecektir