1. FİZİKSEL VE ÇEVRESEL GÜVENLİK

İşyerine yetkisiz erişimlerin engellenmesi ve bilgi varlıklarının hırsızlığa veya tehlikeye karşı korunmasıdır.

Geçmiş zamanlarda önemli bilgiler, taşlara kazılarak daha sonra da kâğıtlara yazılarak fiziksel ortamlarda saklanmış, duvarlarla, kale hendekleriyle ve başlarına dikilen nöbetçilerle koruma altına alınmıştır. Çoğu zaman fiziksel koruma yeterli olmamış ve bilgilerin çalınması ve başka kişilerin eline geçmesi engellenememiştir. Bu durum, verileri korumak için fiziksel güvenliğin tek başına yeterli olmadığını göstermektedir.

Günümüzde de fiziksel güvenlik önemini korumakta ve bu konuyla ilgili gerekli çalışmalar yapılmaktadır. Örneğin, bina etrafına yüksek duvarlar ya da demirler yapılması, bina girişinde özel güvenlik ekiplerinin bulundurulması, önemli verilerin tutulduğu odaların kilitlenmesi ya da bu odalara şifreli güvenlik sistemleri ile girilmesi gibi önlemler kullanılmaktadır.

1.1. GÜVENLİ ALANLAR

Fiziksel Güvenlik Sınırı

- Bilgi işleme servisini korumak amacıyla herhangi bir fiziksel sınır güvenliği tesisi kurulmuş olmalıdır. (kart kontrollü giriş, duvarlar, insanlı nizamiye)
- Fiziksel sınır güvenliği, içindeki bilgi varlıklarının güvenlik ihtiyaçları ve risk değerlendirme sürecinin sonucuna göre oluşturulmuş olmalıdır.

Fiziksel Giriş Kontrolleri

- Kurum içerisinde belli yerlere sadece yetkili personelin girişine izin verecek şekilde kontrol mekanizmaları kurulmalıdır.
- Ziyaretçilerin giriş ve çıkış zamanları kaydediliyor olmalıdır.
- Hassas bilgilerin bulunduğu alanlar (kimlik doğrulama kartı ve PIN koruması gibi yöntemlerle) yetkisiz erişime kapatılmalıdır.
- Tüm personel ve ziyaretçiler güvenlik elemanları tarafından rahatça teşhis edilmelerini sağlayacak kimlik kartlarını devamlı takıyorlar olmalıdır.
- Güvenli alanlara erişim hakları düzenli olarak gözden geçiriliyor olmalıdır.

Ofislerin ve Odaların Güvenliğinin Sağlanması

- Ofisler ve odalarla ilgili fiziksel güvenlik önlemleri alınmalıdır.
- Personel güvenliği ve sağlığı ile ilgili yönetmelikler uygulanmalıdır.
- Kritik tesisler kolayca ulaşılamayacak yerlere kurulmuş olmalıdır.

- Binada bilgi işlem faaliyetlerinin yürütüldüğüne dair işaret, tabela vb. bulunmamasına dikkat edilmelidir.
- Bilgi işlem merkezlerinin konumunu içeren dâhili/harici telefon rehberleri halka kapalı olmalıdır.

Harici ve Çevresel Tehditlerden Korunma

- Yangın, sel, deprem, patlama ve diğer tabii afetler veya toplumsal kargaşa sonucu oluşabilecek hasara karşı fiziksel koruma tedbirleri alınmalı ve uygulanmalıdır.
- Komşu tesislerden kaynaklanan potansiyel tehditler göz önünde bulundurulmalıdır.
- Yedeklenmiş materyal ve yedek sistemler ana tesisten yeterince uzak bir yerde konuşlandırılmış olmalıdır.

Güvenli Alanlarda Çalışma

- Güvenli bir alanın mevcut olduğu ile ilgili olarak veya burada yürütülmekte olan çeşitli faaliyetlerle ilgili olarak personel ve üçüncü parti çalışanları için "İhtiyacı kadar bilme" prensibi uygulanmalıdır.
- Kayıt cihazlarının güvenli alanlara sokulmasına engel olunmalıdır.
- Kullanılmayan güvenli alanlar kilitleniyor ve düzenli olarak kontrol ediliyor olmalıdır.
- Kötü niyetli girişimlere engel olmak için güvenli bölgelerde yapılan çalışmalara nezaret edilmelidir.

Halka Açık Alanlardan, Yükleme ve Dağıtım Alanlarından Erişim

- Bilgi işlem servisleri ile dağıtım ve yükleme alanları ve yetkisiz kişilerin tesislere girebileceği noktalar birbirinden izole edilmiş olmalıdır.

1.2. EKİPMAN GÜVENLİĞİ

Ekipman Yerleşimi ve Koruması

- Ekipman yerleşimi yapılırken çevresel tehditler ve yetkisiz erişimden kaynaklanabilecek zararların asgari düzeye indirilmesine çalışılmalıdır.
- Ekipman, gereksiz erişim asgari düzeye indirilecek şekilde yerleştirilmelidir.
- Kritik veri içeren araçlar yetkisiz kişiler tarafından gözlenemeyecek şekilde yerleştirilmelidir.
- Özel koruma gerektiren ekipman izole edilmiş olmalıdır.
- Nem ve sıcaklık gibi parametreler izlenmelidir.
- Hırsızlık, yangın, duman, patlayıcılar, su, toz, sarsıntı, kimyasallar, elektromanyetik radyasyon, sel gibi potansiyel tehditlerden kaynaklanan riskleri düşürücü kontroller uygulanmalıdır.
- Paratoner kullanılmalıdır.
- Bilgi işlem araçlarının yakınında yeme, içme ve sigara içme konularını düzenleyen kurallar olmalıdır.

Destek Hizmetleri

- Elektrik, su, kanalizasyon ve iklimlendirme sistemleri destekledikleri bilgi işlem dairesi için yeterli düzeyde olmalıdır.
- Elektrik şebekesine yedekli bağlantı, kesintisiz güç kaynağı gibi önlemler ile ekipmanları elektrik arızalarından koruyacak tedbirler alınmış olmalıdır.
- Yedek jeneratör ve jeneratör için yeterli düzeyde yakıt bulundurulmalıdır.
- Su bağlantısı iklimlendirme ve yangın söndürme sistemlerini destekleyecek düzeyde olmalıdır.
- Acil durumlarda iletişimin kesilmemesi için servis sağlayıcıdan iki bağımsız hat alınmış olmalıdır.
- Kurum bu konuda yasal yükümlülüklerini yerine getirmelidir.

Kablolama Güvenliği

- Güç ve iletişim kablolarının fiziksel etkilere ve dinleme faaliyetlerine karşı korunması için önlemler alınmış olmalıdır.
- Kablolar yeraltında olmalıdır.
- Karışmanın ("interference") olmaması için güç kabloları ile iletişim kabloları ayrılmış olmalıdır.
- Hatalı bağlantıların olmaması için ekipman ve kablolar açıkça etiketlenmiş ve işaretlenmiş olmalıdır.
- Hassas ve kritik bilgiler için ekstra güvenlik önlemleri alınmalıdır.
- Alternatif yol ve iletişim kanalları mevcut olmalıdır.
- Fiber optik altyapı yapılandırılmalıdır.
- Bağlantı panelleri ve odalara kontrollü erişim altyapısı kurulmuş olmalıdır.

Ekipman Bakımı

- Ekipmanın bakımı doğru şekilde yapılmalıdır.
- Ekipmanın bakımı, üreticinin tavsiye ettiği zaman aralıklarında ve üreticinin tavsiye ettiği şekilde yapılmalıdır.
- Bakım sadece yetkili personel tarafından yapılıyor olmalıdır.
- Tüm şüpheli ve mevcut arızalar ve bakım çalışmaları için kayıt tutulmalıdır.
- Ekipman bakım için kurum dışına çıkarılırken kontrolden geçirilmelidir.
- İçindeki hassas bilgiler silinmelidir.
- Ekipman sigortalıysa, gerekli sigorta şartları sağlanıyor olmalıdır.

Kurum Dışındaki Ekipmanın Güvenliği

- Kurum alanı dışında bilgi işleme için kullanılacak ekipman için yönetim tarafından yetkilendirme yapılıyor olmalıdır.
- Tesis dışına çıkarılan ekipmanın başıboş bırakılmamasına, seyahat halinde dizüstü bilgisayarların el bagajı olarak taşınmasına dikkat edilmelidir.

- Cihazın muhafaza edilmesi ile ilgili olarak üretici firmanın talimatlarına uyuluyor olmalıdır.
- Evden çalışma ile ilgili tedbirler alınmış olmalıdır. Sigorta cihazların tesis dışında korunmasını kapsıyor olmalıdır.
- Kurum alanı dışında kullanılacak ekipmanlar için uygulanacak güvenlik önlemleri, tesis dışında çalışmaktan kaynaklanacak farklı riskler değerlendirilerek belirlenmiş olmalıdır.

Ekipmanın Güvenli İmhası ya da Tekrar Kullanımı

- Ekipman imha edilmeden önce gizli bilginin bulunduğu depolama cihazı fiziksel olarak imha edilmelidir.
- Depolama cihazının içerdiği bilginin bir daha okunamaması için klasik silme veya format işlemlerinin ötesinde yeterli düzeyde işlem yapılmalıdır.

Varlıkların Kurumdan Çıkarılması

- Ekipman, bilgi veya yazılımın yetkilendirme olmadan tesis dışına çıkarılmamasını sağlayan kontrol mekanizması oluşturulmuş olmalıdır.
- Kurum varlıklarının yetkisiz olarak kurum dışına çıkarıldığını saptamak için denetleme yapılmalıdır.
- Kurum çalışanları bu tip denetlemelerden haberdar olmalıdır.