1. AMAÇ

Bu politika, Karamanoğlu Mehmetbey Üniversitesinin Bilgi İşlem Daire Başkanlığı Fiziksel ve Çevresel Güvenlik ilkelerini oluşturmayı amaçlamıştır.

2. KAPSAM

Bu politika, Karamanoğlu Mehmetbey Üniversitesi Bilgi İşlem Daire Başkanlığı Fiziksel ve Çevresel Güvenlik tedbirlerini kapsamaktadır.

3. SORUMLULAR

- Bilişim Sistemi Kullanıcıları
- Bilgi İşlem Daire Başkanlığı

4. TANIMLAR

5. UYGULAMA

5.1 Fiziksel ve Çevresel Güvenlik

5.1.1 Fiziksel Güvenlik Kapsamı

Kurumun, Bilgi İşlem, İşlem donanımlarını içeren ofislerinin mantıksal olarak farklı fiziksel bölgelere ayrılması gereklidir. Her bölge, kendine uygun erişim kısıtlamaları ve erişim yetkilendirmelerine sahiptir. Kritik Bilgi İşlem donanımı barındıran bölgeler, "Güvenli Alan" olarak tayin edilir.

5.1.2 Fiziksel Giriş Kontrolleri

Kurum binasına giren tüm ziyaretçi ve tedarikçiler için kimlik kontrolü, eşya ve çantalarının kontrol edilmesi gibi uygun güvenlik kontrolleri uygulanır. Binaya sokulan ya da binadan çıkartılan malzemelerin tüm hareketleri gerektiği şekilde onaylanır ve takip edilir. (Bilgi Güvenliği Prosedürleri "Bina Giriş Kısıtlamaları")

5.1.3 Ofislerin, Odaların ve Tesislerin Güvenliğinin Sağlanması

İçlerinde barındırdıkları hassas bilgiye göre ofisler, odalar ve tesisler için fiziksel güvenlik kontrolleri tasarlanır ve uygulanır. Sistem odasına erişim kısıtlanır. Yalnızca Bilgi İşlem Müdürlüğü personeli ve Bilgi İşlem Müdürü tarafından onaylanmış yetkili kişiler sistem odasına erişim hakkına sahiptirler. (Bilgi Güvenliği Prosedürleri "Dış ve Çevresel Etkenlere Karşı Koruma"),

5.1.4 Dış ve Çevresel Tehditlere karşı Koruma

- Kurum binalarının kritik noktaları, Kurum kaynaklarının oluşacak herhangi bir yangında zarar görmemesi için uygun yangınla mücadele araçlarıyla donatılır.
- Düzenli olarak yangın ve deprem tatbikatları gibi güvenlik uygulamaları gerçekleştirilir.
- Kuruma ait binalarda su baskını ya da uygun olmayan tahliye sisteminden ötürü kayıp veya hasar meydana gelmemesi için uygun güvenlik önlemi alınır.
- Doğal veya insan kaynaklı felaketlerden kaynaklanacak hasardan korunmak için fiziksel önlemler tasarlanıp uygulanır. (Bilgi Güvenliği Prosedürleri "Dış ve Çevresel Etkenlere Karşı Koruma")

5.1.5 Güvenli Bölgelerde Çalışma

Güvenli bölgelerde çalışılması için fiziksel koruma ve kılavuzlar sağlanır. (Bilgi Güvenliği Prosedürleri "Güvenli Bölgelerde Çalışma")

5.1.6 Genel Erişim, Sevk ve Yükleme Alanları

Sevk ve yükleme alanları gibi yetkisiz kişilerin binalara girebileceği noktalar kontrol altında tutulur ve bilgi işlem tesislerinden izole edilir. (Bilgi Güvenliği Prosedürleri "Genel Erişim, Sevk ve Yükleme Alanları")

5.1.7 Donanımın Yerleştirilmesi ve Korunması

Faks, yazıcı dâhil tüm elektronik ofis donanımlarının fiziksel güvenliği sağlanır.

Masaüstü bilgisayar güvenliği ve ağ cihazları

- Masaüstü bilgisayarlar ve her tür bilgisayara ait donanım uygun şekilde yangın, su, kirlilik ve voltaj yükselmelerine/düşümlerine karşı korunur.
- Ağ cihazları yangına, ısıya, toza ve suya karşı korunur.
- Ağ kablolarındaki kesikler ya da hasarlar kontrol edilir ve bunlar için önlemler alınır.

Ortam Yönetimi ve Güvenlik

- Elektronik saklama ortamları, yangın, nem ve manyetik alan gibi sebeplerden ötürü oluşabilecek fiziksel hasarlara karşı korunur.
- Elektronik ortam envanteri tutulur.
- Elektronik ortamlar, bu ortamlara ihtiyaç kalmadığında güvenli ve emniyetli bir şekilde imha edilir. Hassas ve gizli bilginin yetkisiz kişilerin eline geçme riskini en aza indirmek için, elektronik ortamların güvenli imhalarını sağlayacak prosedürler uygulanır.

Yardımcı Donanımlar

- Donanımlar, güç kesintilerinden ve yardımcı donanımlarda meydana gelen arızaların sebep olacağı aksaklılardan korunur.
- Kurum bünyesinde düzenli güç kaynağı sağlayabilecek bir donanım sağlanır. Ana güç kaynağının kesilmesi durumunda sürekli güç sağlayabilecek alternatif güç kaynakları hazırda bulundurulur.
- Kablolama Güvenliği

Veri taşıyan veya yardımcı bilişim hizmetlerine hizmet eden güç ve haberleşme kabloları hasar görmeyecek ya da hasara uğratılamayacak şekilde korunur.

5.1.8 Donanım Bakımı

Tüm donanımlar, sürekli erişilebilirlik ve bütünlüğün sağlanması amacıyla uygun şekilde yönetilir ve bakımlarının yapılması sağlanır.

5.1.9 Bina Dışındaki Donanımların Güvenliği

Tesis dışına çıkarılan donanım için (dizüstü vb.) maruz kalabileceği riskler düşünülerek gerekli güvenlik önlemleri alınır.

5.1.10 Donanımların Güvenli İmhası ve Tekrar Kullanımı

Bilgi İşlem donanım ve ekipmanları artık kullanılmayacaksa onay alındıktan sonra imha edilir. İmhadan önce, donanımların üzerindeki veriler uygun yöntemlerle silinir. Kullanılmayan donanım ve elektronik ortamların imhası mevcut çevre, yasa ve yönetmeliklerine uygun olarak gerçekleştirilir.

5.1.11 Bilgi Varlıklarının Taşınması

Her tür Donanım, bilgi veya yazılım, onay alınmadan hiçbir koşulda bina dışına çıkarılmaz. Bilişim Teknolojileri ile ilgili Donanım, bilgi veya yazılım Bilgi işlem müdürlüğü onayı alınmadan yeri değiştirilemez.

6. İLGİLİ DOKÜMAN

- Fiziksel ve Çevresel Güvenlik Prosedürü
- Erişim Kontrolü Prosedürleri
- Bilgi Saklama Ortamları Yok Etme Prosedürü