1. AMAÇ

Bu prosedür, Karamanoğlu Mehmetbey Üniversitesi Bilgi İşlem Daire Başkanlığı Fiziksel ve Çevresel Güvenlik kurallarının yapılması amaçlanmıştır.

2. KAPSAM

Bu prosedür, Karamanoğlu Mehmetbey Üniversitesi Bilgi İşlem Daire Başkanlığı bünyesinde yapılan Fiziksel ve Çevresel Güvenlik önlemlerini kapsar.

3. SORUMLULAR

- Bilgi İşlem Daire Başkanlığı
- Bilişim Kullanıcıları

4. TANIMLAR

5. UYGULAMA

5.1 Fiziksel Güvenlik Kapsamı

Kurum'un Bilgi İşlem donanımlarını içeren ofisleri mantıksal olarak farklı fiziksel bölgelere ayrılır. Her bölge, kendine uygun erişim kısıtlamaları ve erişim yetkilendirmelerine sahiptir. Kritik Bilgi İşlem donanımı ve bilgi varlıklarını toplu olarak barındıran bölgeler, güvenli bölge olarak tayin edilir.

Kurum'un ofisleri aşağıdaki güvenlik bölgelerine ayrılır:

1. Bölge:- Bina girişi, lobi
2. Bölge:- İş Birimlerinin çalıştığı ofisler
3. Bölge:- Bilgi İşlem Sistem odası

5.2 Bina Giriş Kısıtlamaları

Bina içerisindeki girişler, personelin bina içerisinde tanımlanmış rolüne göre kısıtlanır. Sistem odası mahiyetindeki bölgelere erişimler ayrıca yetkilendirmeye tabidir. Sunucu odasına erişim yetkisi sadece Bilgi İşlem Bölümü personelindedir. Kısıtlama, parmak izi okuyucu sistemi ile gerçekleşir. Operasyon merkezi mahiyetindeki bölgelere erişim yetkisi ilgili bölüm çalışanları ve bina güvenlik birimi ile sınırlı tutulur. Kısıtlama, şifreli giriş sistemi ile gerçekleşir.

5.2.1 Çalışanlar için Giriş Kısıtlamaları

Çeşitli güvenlik bölgelerine giriş, organizasyon içerisinde tanımlanmış rollere göre kısıtlanır. Kısıtlama, şifreli erişim sistemi ile gerçekleşir. 2. Güvenlik Bölgeleri'ne erişimi sağlayacak şifre, İK Birimi ve fiziksel güvenlikten sorumlu bölüm yöneticisinden talep edilir. 3. Güvenlik Bölgeleri'ne erişimler ise Bilgi İşlem Yöneticisi'nin izni ile yetkilendirilir. Giriş,

24 saat güvenlik görevlileri tarafından gözetlenir ve korunur. Güvenlik görevlileri, tüm ziyaretçilere kimliklerini sorar, ziyaretçi bilgilerini, giriş ve çıkış saatlerini kayıt altına alır ve ziyaretçilere bina içerisinde gitmesi gereken yere kadar refakat eder ya da ziyaretçiyi karşılaması için görüşmeye geldiği kişiyi bilgilendirir. Ziyaretçiler tesis içerisinde refakatsiz dolaşamaz. Güvenlik bölgelerine erişimler, tüm çalışanlar için bilinen ihtiyaçlar temel alınarak temin edilir. Giriş yaparken tüm çalışanlar şifre ile erişim sağlar.

5.2.2 Ziyaretçiler için Giriş Kısıtlamaları

Kurum yönetimi kuruluş dışından gelen kişilerin girişine aşağıdaki durumlarda giriş izni tanımlamalıdır: Ziyaretçiler; ziyaretçi, tedarikçi, kontratlı çalışan, danışman, denetçi, çalışan adayı şeklinde tanımlanabilir. Daha önceden ziyaret bilgisi güvenliğe bildirilmemiş ziyaretçiler için (kişisel nedenler, ziyaret vs.) binaya giriş öncesinde, ilgili bölümden yazılı izin alınır. Ziyaretçiler, hassas bilginin veya verinin saklandığı sistem odası veya fiziksel bölgelere girecekse ziyareti gerçekleştirmeden önce ziyaretçiyi davet eden birim tarafından ilgili alanın sorumlusundan (örn. Sistem odası için Bilgi İşlem yöneticisinden) yazılı izin alır. Hassas bilginin veya verinin tutulduğu bu bölgeleri ziyaretler sırasında ziyaretçilere her zaman refakat edilir. Düzenli danışmanların ve tedarikçilerin kaydı ayrı bir liste olarak tutulur ve kapı giriş çıkışlarının kontrolünden sorumlu bölüm, bu kişilerin binaya girişinden önce kişilerin isimlerini ve kimliklerini doğrular. Bu kişiler, binadan çıkarken tekrar kontrol edilir ve kayda geçen eşyalar dışında bir malzemenin dışarıya çıkarılmadığından emin olunur. Ziyaretçiler hafta sonları ve tatillerde çalışabilmek için ilgili bölümden yazılı izin alır. Bu çalışmaya ilgili bölümden en az bir sorumlu refakat eder.

5.3 Sistem Odası Erişimi

Sistem odasına erişim parmak izi okuyucu sistem kontrolleri ile kısıtlanır. Erişim hakkı Bilgi İşlem bölümünün belirli çalışanlarına veya bina idaresi tarafından güvenlik için uygun görülen kişilere tanınır. Erişim yetkisini Bilgi İşlem Yöneticisi onaylar. Her ay çeşitli personele atanmış erişim yetkileri Bilgi İşlem Yöneticisi tarafından gözden geçirilir. Hizmet sağlayıcılar, Bilgi İşlem donanımının veya Bilgi İşlem altyapısının bakımı için sistem odasına girdiğinde ya da sistem odasının temizlenmesi sırasında nezaretçiler bu kişilere refakat eder ve yapılan işin tümü bu kişilerin nezaretinde yapılır. Hiçbir 3. tarafın, Kurum Bilgi İşlem personelinin nezaretinde olmaksızın sistem odasına girmesine izin verilmez. Veri merkezine ve operasyon bölgesine kör nokta bırakmayacak şekilde güvenlik kameraları tesis edilir ve bu bölümler yetkin güvenlik personeli tarafından izlenir ve görüntüler kayıt altına alınır. Bu kayıtlar denetlenir ve diğer giriş kayıtları ile bağlantısı kurulur. Görüntü kayıtları an az 20 gün saklanır. Kamera sisteminin saati, merkezi sistem saati ile aynıdır. Tüm sistem odası girişlerinin tutulduğu elektronik denetim izleri en az bir sene boyunca saklanır. Bu prosedürler tüm ofislerde bulunan sistem odaları için geçerlidir.

5.4 Dış ve Çevresel Tehditlere Karşı Korunma

Bkz. Çevresel Güvenlik Standartları

5.5 Güvenli Bölgelerde Çalışma

Kurum personeli bir güvenli bölgenin varlığından ve bu bölgede gerçekleşen faaliyetlerden sadece gerekli görüldüğü durumlarda haberdar olur. Güvenli alanlarda, sorumlu bir çalışan tarafından gözetim altına alınmayan çalışmalardan kaçınılır. Çalışılmayan güvenli bölgeler fiziksel olarak kilitlenir ve periyodik olarak kontrol edilir. Mobil cihazlardaki bütünleşik kameralar gibi fotoğraf, video, ses veya diğer kayıt cihazlarının kullanımına, Bilgi İşlem Şube Müdürünün veya Bilgi Güvenliği Yöneticisi'nin onayı olmadan izin verilmez.

5.6 Genel Erişim, Sevk ve Yükleme Alanları

Sevk ve yükleme alanlarına bina dışından erişim, belirlenmiş ve yetkilendirilmiş personel ile sınırlıdır. Sevk alanı, sevk personelinin sevk işlemi esnasında binanın başka bölümlerine erişemeyeceği şekilde tasarlanmıştır. Sevk ve yükleme alanlarının iç kapılarının açık olması durumunda dış kapıların güvenliği sağlanır. Gelen malzeme, sevk ve yükleme alanlarından kullanılacağı yere taşınmadan önce, potansiyel tehditlere karşı incelenir. Gelen malzeme, bölgeye girişi esnasında varlık envanter prosedüründe belirttiği şekilde kayıt altına alınır. Mümkün olduğu yer ve durumlarda, gelen ve giden sevkiyatlar birbirinden ayrılır.

5.7 Donanımın Yerleştirilmesi ve Korunması

Hassas verinin tutulduğu ya da işlendiği sistemlerin bulunduğu yerler yetkisiz kişilerin erişebileceği ya da görebileceği yerlere konumlandırılmaz. Özel koruma gerektiren malzemeler, gerekli koruma seviyesi için izole edilir.

5.8 Elektronik Ofis Donanımlarının Güvenliği

Faks, yazıcı ve ofis telefon sistemi gibi elektronik ofis donanımları alıcı ortam olduklarından veya fiziksel ya da ses formatındaki veriyi işlediklerinden, fiziksel güvenliği sağlanması gereken ekipmanlardır. Bu donanımlarla ilgili güvenlik kaygıları şu şekildedir: Faks ve yazıcılar gibi cihazların Kurum çalışanlarının görüş alanı içerisinde bulunan güvenli bir bölgeye yerleştirilmesine dikkat edilir. Bunlara erişim, çalışanların farkına varmadan bir ziyaretçinin kolayca erişemeyeceği şekilde kısıtlıdır. Faks ve yazıcı sorumluları fiziksel erişim güvenliğini sağlar ve gerekli önlemleri alır. Bu donanımlar, ısıdan, kirlilikten ve diğer çevresel tehlikelerden korunur. Katlarda bulunan ofis yazıcıları, fiziksel sınırlamalar sebebi ile ayrı bir güvenli ortamda bulundurulamayacaksa, bu cihazlardan alınacak çıktıların güvenliği sağlanır. Faks, yazıcı ve ofis telefon sistemi güvenli bir bölgede konumlandırılır, kurumun önemli araçlarından biridir ve yetkisiz erişim ve diğer çevresel tehditlere karşı korunur. Kime ait olduğundan bağımsız olarak, her tür bilgi işlem donanımının bina dışında kullanılma yetkisi yönetim tarafından onaylanır. Bina dışına çıkarılan donanım ve veri saklama ortamı, kamuya açık alanlarda gözetimsiz bırakılmaz.

5.9 Masaüstü ve Dizüstü Bilgisayarların Fiziksel Güvenliği

Bütün kullanıcılar, kendilerine verilen her masaüstü ve dizüstü bilgisayarın fiziksel güvenliğinden sorumludur. İlgili kullanıcılar, masaüstü ve dizüstü bilgisayarların, ateş, su ve kirliliğe karşı güvenliğinden sorumludurlar. Bu kişilerin sorumlulukları, güvenliği sağlamak için her türlü önlemi almak ve bir problem/olay ile karşılaşılması durumunda fiziksel güvenlik

birimine bilgi vermektir. Dizüstü bilgisayarlar, kullanıcının ofis binası dışına çıkması gerektiği durumda masaya kilitlenir veya kilit altında tutulur. Bu uygulamanın gerçekleştirilemediği durumlarda, Kurum tarafından bu cihazların veri depolama birimlerinde (örn. Hard disk) bulunan bilgilerin hırsızlık tehdidine karşı korunması amacıyla şifrelenmesi sağlanır.

5.10 Ağ Dağıtıcılarının (Hub& Switch) Fiziksel Güvenliği

Bina içerisindeki ağ dağıtıcıları kilitli kabinlerde tutulur ve yangın, ısı, toz ve sudan korunur. Tüm ağ girişleri (network jacks) ve erişim noktaları sadece yetkili çalışanlar tarafından erişilebilirdir. Kurum ağ dağıtıcı cihazların fiziksel güvenliğinin sağlanması için gerekli önlemleri almak veya aldırmaktan sorumludur.

5.11 Yardımcı Donanımlar

Bkz. Çevresel Güvenlik Standartları

5.12 Kablolama Güvenliği

Güç ve veri taşıyan veya bilgi sistemlerini destekleyen haberleşme kabloları hasar veya dinlenmeye karşı korunur. Şu hususlar göz önünde bulundurulur:

- Binaya ve sistem odasına giren güç ve haberleşme hatları zeminin altından geçirilir veya uygun biçimde korunur.
- Ağ pasif elementleri, yetkisiz müdahaleye veya hasara karşı kablo kanalları/boruları kullanılarak korunur.
- Güç kabloları, girişimi engellemek için iletişim kablolarından ayrılır.

5.13 Elektronik Ofis Donanımlarının Bakımı

Tüm donanımların bakımı, tedarikçinin önerdiği sıklıkta ve şekilde yapılır. Sadece yetkili servis personeli tamir ve servis işlemlerini gerçekleştirir. Şüphelenilen veya karşılaşılan tüm hataların, önleyici ve düzeltici bakım işlemlerinin kayıtları tutulur. Bakım zamanı belirlendiğinde, bu bakım işleminin kuruluş çalışanları ya da üçüncü taraflar tarafından yapılıp yapılmayacağına göre uygun kontroller gerçekleştirilir; mümkün olduğu durumlarda, kritik bilgi donanımlardan temizlenir veya servis personeli tarafından gerektiği şekilde temizlenir. Yapılan bakımlar tarih ve kontrol ayrıntılarını içerecek şekilde kayıt altına alınır.

5.14 Bilgi İşlem Donanımı Yönetimi

Sistem yöneticileri sunucuların yönetiminden, Kurum bünyesinde çalışan ağ yönetimi ekibi de ağ donanımlarının yönetiminden sorumludur.

5.14.1 Önleyici Bakım

Önleyici bakım, sunucu ve ağ donanımlarına kesintisiz erişilebilirlik için gerekli olan, Bilgi İşlem donanımları üzerinde gerçekleştirilen önemli bir işlemdir.

Tipik bakım faaliyetleri şunlardan oluşur:

- Sabit disk kapasitesinin kontrol edilmesi, dosyaların birleştirilmesine yönelik tüm lokal sabit disklerin optimize edilmesi ve disk yüzeylerinin bozuk sektörlere yönelik taranması
- Geçici dosyaların ve yedeklenen denetim izi dosyalarının temizlenmesi
- Düzenli temizliğin sürdürülmesi (tozdan arındırma, döküntü ve kirliliğin ortadan kaldırılması vs.) ve kablolama bütünlüğünün düzenli kontrol edilmesi (kablo sonlarının eklentileri, fazla kablo uzantılarının sarılması, düzenli kablo yolları, temiz kablo bağlantıları)
- Batarya tertibatının bakımı, güç kablolarının bağlantılarının düzgünlüğü, topraklama uçlarının ve kablo yollarının düzgünlüğü ve bütünlüğü, muhafaza şaşısının bütünlüğünü içeren UPS Güvenliği vs.
- Vida ve cıvataların sıkılığı, donanımın bir yerden bir yere kaydırılması anındaki dikkat ve buradaki yardımcı bağlantıların kontrolünü içeren fiziksel kurulum bütünlüğü

Bakım faaliyetleri, donanım ve hizmeti sağlayan kişilere göre farklılık gösterebilir. Sistem yöneticileri ve ağ yöneticileri tüm Bilgi İşlem donanımının bakım gereksinimlerini belirler ve önleyici bakım programını belirler. Satın alma anlaşmasının bir parçası olarak bir kısım donanım için, satıcılar önleyici bakımları sağlar. Bu bakım programı kurum'un kendi gerçekleştirdiği bakımlara ilişkin programına eklenir. Sistem ve ağ yöneticileri hazırlanan önleyici bakım programına göre bakımları gerçekleştirirler. Bilgi İşlem yöneticisi, sistem ve ağ yöneticileri, tarafından sürdürülen bakım faaliyetlerini ayda bir defa gözden geçirir. Bilgi Güvenliği Yöneticisi, bakım hizmetini sağlayan tarafların ve yöneticilerin bakım programına uyduğunu kontrol eder. Tüm bakım faaliyetleri için yöneticiler: Önleyici bakım programının ve bu kapsamdaki faaliyetlerin kritik veya hassas uygulamaları aksatmamasını ve herhangi bir şekilde etkilememesini, Bakım faaliyetlerinin, verinin yoğun olarak işlendiği kritik dönemler ve yedekleme veya geri yükleme gibi diğer Bilgi İşlem faaliyetleri ile çakışmamasını ve

Tüm taraflara herhangi bir bakım faaliyeti öncesinde bilgi verilmesini sağlar.

5.15 Bilgi İşlem harici Donanımların (Ofis-Ekipman) Yönetimi

Faks, fotokopi makineleri, yazıcılar gibi cihazlar Kurumun günlük operasyonların yönetilmesi için önemli araçlardır. Bu donanımların sürekli olarak doğru şekilde çalışması şu yöntemlerle sağlanır: Tüm ofis donanımları kullanıcılarına bu donanımları doğru şekilde kullanabilmeleri için uygun eğitimler verilir. Kullanıcılar ofis ekipmanlarını kullanım kılavuzlarında açıklandığı şekilde kullanırlar. Fotokopi makineleri ve diğer donanımlar için bakım sözleşmeleri bulunur. İlgili görevliler her mesai başlangıcında, faks makinelerinin, fotokopi cihazlarının ve kritik yazıcıların durumlarını ve doğru çalıştıklarını kontrol eder. Eğer kartuşlar boşalmak üzereyse, yedek kartuşlar hazırlanır. Bakım işlerinden sorumlu bölüm yöneticisi, donanımlar için mevcut bakım sözleşmeleri göz önünde bulundurarak bir bakım programı hazırlar. Bu bakım programının kapsamında, her bir faks makinesi, tarayıcı, fotokopi cihazı, yazıcı, klima ve UPS'in belli aralıklarla doğru çalıştığı kontrol edilir. İlgili bölüm, donanımların önleyici bakımlarının bakım sözleşmelerine göre yapılmasını sağlar. İlgili bölüm yöneticisi, bakım programını ve bakım sonuçlarını ayda bir defa gözden geçirir.

5.16 Bina Dışındaki Donanımların Güvenliği

- Kime ait olduğundan bağımsız olarak, her tür bilgi işlem donanımının bina dışında kullanılma yetkisi yönetim tarafından onaylanır.
- Bina dışına çıkarılan donanım ve veri saklama ortamı kamuya açık yerlerde her zaman gözetim altında tutulur.
- Seyahat sırasında taşınabilir bilgisayarlar el bavulunda ve mümkünse dışarıdan belli olmayacak şekilde taşınırlar.
- Üreticinin donanımın korunmasına yönelik talimatlarına her koşulda uyulur.
- Donanımı saha dışında koruyacak seviyede sigorta yaptırılmıştır.

5.17 Veri Depolama Ortamlarının İmhası

Saklama ortamları, kullanımına ihtiyaç olmadığında güvenli ve tehlikesiz şekilde imha edilir. Saklama ortamları yeterli özen gösterilmeden imha edildiğinde, hassas bilgi başka kişilerin eline geçebilir. Riski en aza indirmek amacıyla veri depolama ortamlarının güvenli imhası için resmi prosedürler hazırlanır. Aşağıdaki esaslar değerlendirilir:

Hassas bilgi ve lisanslı yazılım içeren saklama ortamları güvenli ve tehlike içermeyecek şekilde saklanır ve imha edilir (yakarak, parçalara ayırarak, kuruluş içerisinde başka bir uygulama tarafından kullanılmadan önce bilgi işlem müdürlüğü çalışanları tarafından format atılarak, anlaşmalı kurumlar aracılığı ile vb.).

Aşağıdaki liste güvenli imhası gereken malzemeleri listelemektedir:

- Kâğıt dokümanlar
- Ses veya diğer kayıtlar
- Çıktı raporları
- Manyetik kasetler
- Çıkarılabilir disk ve kasetler
- Optik depolama ortamları (tüm formlar ve yazılım dağıtıcı ortamlar da dahil)
- Program dökümü
- Test verisi
- Sistem dokümantasyonu
- Hassas malzemelerin imhasına yönelik denetim kaydı tutulur.

İmha için malzeme toplanması sırasında, gizli olarak nitelendirilmeyen bilginin miktarı artarak bir grup gizli bilgiden daha hassas ve daha kritik bir hale dönüşebilir. Bu yığın etkisine özel olarak dikkat edilmelidir.

5.18 Varlıkların Bina İçine ve Dışına Taşınması

5.18.1 Bina Dışına Malzeme Taşınması

Dışarı çıkartılan tüm malzemeler için Bilgi İşlem yönetimi tarafından onay temin edilir. Dışarı çıkarılacak bu malzemeler Bilgi İşlem yönetimi tarafından gizlilik derecesine göre ve gerek gördüğü durumlarda kayıt defterinde tutulur ve takip edilir. Güvenlik sorumluları gerekli gördükleri durumlarda, dışarıya çıkartılan malzeme için Bilgi İşlem yönetiminin onayını kontrol etmekle mükelleftir. Eğer bir Bilgi İşlem varlığı tamir için dışarıya çıkartılıyorsa, muhtemel dönüş tarihi de tutulan kayıtlara eklenir. Çıkışı yapılan varlığın bir hafta içerisinde geri getirilmemesi halinde, bu gecikmeden Bilgi İşlem yönetimi haberdar edilir ve hizmeti sağlayan taraftan açıklama temin edilir (Envanter Kayıtları envanter listesinden kontrol edilebilir).

5.18.2 Bina İçine Malzeme Taşınması

- Güvenlik personeli binaya girişi yapılan malzeme ile ilgili bilgi toplar ve malzemenin binada ilgili birime iletilmesini sağlar.
- İlgili çalışan, malzemenin teslim alındığına dair bilgilendirilir.
- Malzemeyi teslim alan çalışan ilk incelemeyi yapar ve bir problem olmaması durumunda malzemenin girişini onaylar.
- İlgili çalışan da ayrıca, malzemenin alındığına dair bilgileri envanter listesine girer.

5.19 Çevresel Güvenlik Standartları

5.19.1 Güç Kaynağı

Güç kaynağı, Kurum'un iş sürekliliği açısından kritiktir. Güç kaynağı düzenlemeleri şu şekilde yapılır:

Yerel Güç Kaynağı

Yerel elektrik sağlayıcılardan gelen elektrik kaynağı değişmediğinden, operasyon bölgesinin beslendiği elektriği yerel bir dönüştürücü üzerinden 220-250V değerini geçmeyecek şekilde ayrıca, sistem odası içerisinde kullanılan gerilim, sunucuların kılavuzlarında belirtilen değerlere uygun olacak şekilde düzenlenir. Donanımın hat gerilimindeki aşırı artıştan korunması için uygun kapasiteli güç kesiciler kullanılır.

Kesintisiz Güç Kaynağı (UPS)

Sistem odasına ve sunuculara tahsis edilmiş, bakım istemeyen (tedarikçi tarafından belirtilen sıklıkta yenisi ile değiştirilmesi gereken) bataryaya sahip bir UPS bulundurulur. UPS ideal olarak sistem odasında veya toz içermeyen benzer bir ortamda bulundurulur. UPS etrafında bakıma imkan verecek kadar geniş bir alan bırakılır. UPS, ana güç kaynağının sağladığı

gerilimi sağlayacak düzeyde olur ve devreye giren UPS'in işleyişinde herhangi bir hata/arıza olmaz.

UPS'in bulunduğu odada, sürekli olarak, UPS işletme talimatlarını gösteren bir çizim bulundurulur.

UPS ve jeneratör, sistem odası güç kaynağının doğru çalıştığının kontrol edilmesi amacıyla düzenli olarak test edilir.

Jeneratör

Jeneratör, yerel güç kaynağı kesilir kesilmez devreye girecek şekilde otomatik hale getirilir. Tüm bakımları, Sistem İşletme Müdürlüğü ve ilgili birimler tarafından yapılır.

Test

UPS ve jeneratör, sistem odası güç kaynağının doğru çalıştığının kontrol edilmesi amacıyla düzenli olarak ilgili birimler tarafından test edilir.

5.19.2 Sıcaklık ve Hava Kirliliği

Bilgi İşlem donanımlarını etkileyebilecek tozun, ısının ve hava kirliliğinin kontrol altında tutulması için klima kullanılır. Sıcaklık ve nem ölçen cihazların kalibrasyonu yapılır, alarmların minimum ve maksimum değerleri incelenir.

Sıcaklık

Sistem odasında, odanın sıcaklığını 20 derecenin altında tutacak uygun özellikte ve sayıda klima bulundurulur.

Nem

Sistem odasındaki nem seviyesi %50'nin üzerine çıkamaz. Sistem odasında, bir nem izleme sistemi veya bir nem aygıtı bulunur.

5.19.3 Toz

Sistem odasında tozdan oluşabilecek zararları önlemek amacıyla iklimlendirme cihazları kullanılır. Ayrıca sistem odasının periyodik temizliği, sistem odası sorumlularının refakati dâhilinde gerçekleştirilir.

5.19.4 Yangın Güvenliği

Sistem Odası:

- Sistem odası, tepkimesiz gaz içeren yangın söndürücü sistem ile donatılır.
- Yangının tespit edilmesinin ardından yangın alarmı 30 saniye boyunca çalışır ve yangın söndürücü sistem otomatik olarak devreye girer. Personel, belirtilen 30 saniyelik zamanı sistem odasını boşaltmak için kullanır.
- Yangına dayanıklı kapılar, sistem odasını odanın dışındaki bir yangına karşı korur.

Yangın Alarmları:

- Tüm bina yangın alarmıyla donatılır.
- Yangın detektörünün yangını tespit edemediği durumlarda çalışanlar tarafından kullanılmak üzere, binanın stratejik noktalarında manüel alarmlar bulunur.

Yangınla Mücadele Yöntemleri:

- Yangına neden olan ısı düşürüldüğünde artık yangını devam ettirmeye yetecek ısı ortadan kalkmış ve yangın kontrol altına alınmış olur.
- Bu aşamada su yangını söndürmek için kullanılır. Bu yönteme, yanan malzemenin ahşap, kâğıt vb. olması durumunda başvurulabilir.
- Yangın, etrafta yanıcı malzemeler bulunduğu sürece devam edecektir. Dolayısıyla, yangın, bu tip malzemelerin ortamdan çıkarılması durumunda kontrol altına alınabilir.
- Eğer yanmakta olan cismin yeri fiziksel olarak değiştirilebiliyorsa, yangın kolayca kontrol altına alınır. Mümkün olmadığı durumlarda çevredeki diğer yanıcı maddeler yangının etkisindeki bölgeden uzaklaştırılır.
- Yangın söndürme ekipmanları bina içerisinde her katta bulunur ve çalışanlar düzenli olarak bu ekipmanları kullanabilmelerini sağlayacak eğitimleri alırlar.

Acil Durum Çıkışları:

- Acil durum çıkışları veya Tahliye güzergâhları bina içerisinde açıkça görülebilecek şekildedir.
- Bina içerisinde, herhangi bir materyalin çıkışını veya güzergâhları engelleyecek ya da zorlaştıracak şekilde konumlandırılmazlar. Senede en az bir defa yangın tatbikatı gerçekleştirilir.

Yangın durumunda yapılacaklar:

- Yangın başlar başlamaz, en hızlı şekilde yangın alarmını aktive etmek.
- Yangın söndürülemiyorsa, yardım için seslenmek; Yangın söndürme ekibine ve güvenlik birimine hemen haber vermek ve İlgili Bölüm Yöneticisine danışmak ve yangın müdahale ekibi tarafından verilen talimatlara uymak.

Alarm aktive edildiğinde:

- Bir acil durum ekibi zemin katta, yangın, hırsızlık ve bombalı saldırı tehdidi gibi durumlara müdahale etmek için hazır bulunur.
- Bu ekip yangın alarmının başlamasıyla en hızlı şekilde müdahaleye hazırlanır.
- Öncelikle sorumlu ekip yangın alarmını kontrol eder.
- Yangın söndürme ekibi çalışanları yangından haberdar etmek ve yangın esnasında onları yönlendirmekle sorumludur.
- Personel, değerli dokümanları ve evrakları dolaplara kilitler ve binayı tahliye eder.
- Yangın müdahalesine yönelik talimatlar, yangının tipine, ortaya çıktığı yere göre farklılık gösterecektir.
- Yangın alarmı durumu çalışanların maksimum işbirliğini gerektirir.
- Kurum binasında bulunan çalışanlar ve müşteriler sakin kalmalı ve yangın söndürme ekibinin talimatlarına göre hareket etmelidir.

Yangın söndürme ekibi için talimatlar:

- Seçilmiş çalışanlar, yangın söndürme ekibine dâhil edilir ve bu kişiler yangın söndürme teknikleri üzerine eğitilirler.

- Yangın söndürme ekibi, ani bir yangın durumunda, yangınla mücadele prosedürlerinde yer alan bilgileri uygular.
- Yangın kontrol altına alınamayacaksa, yangın alarmı çalıştırılır.
- Soğukkanlılık korunur ve kattaki herkesin tahliyesini sağlayacak düzenlemeler yapılır.
- Hastalık ve çeşitli sebeplerden ötürü yürüyemeyecek durumdaki kişilerin, sorumlu ekip tarafından, zemin kata ya da güvenli bölgelere götürülmeleri gerekir.
- Yangın söndürme ekibi, kendileri bulundukları katı terk etmeden önce herkesin çıkmış olduğundan emin olur. Bulunamayan kişiler güvenlik personeline bildirilir.

Bina çalışanlarının sorumluluğu:

- Hayat kurtarma yolları ve yöntemleri bulmak,
- Yangın alarmını çalıştırmasını öğrenmek,
- Yangın söndürme ekipmanlarını doğru şekilde kullanmayı öğrenmek.

Şunlardan kaçınılır: Hayat kurtarmak amacıyla binayı tahliye etmek için asansörü kullanmak, Bağırmak ve kargaşa yaratmak – Bu şekilde insanlar daha dikkatsiz olacaklardır,

Kişisel eşyaları kurtarmak için beklemek camın kırılması ile oluşan yangın alarmları ve yangın söndürme vanaları her katın girişine konulur. Bununlar beraber, aşağıdaki yangınla mücadele ekipmanları da her katta mevcuttur:

- Suyla müdahale için olan ekipmanlar,
- Duman algılayıcılar her katta bulunur ve bu algılayıcılar duman algılandığında derhal duman alarmını aktive eder.
- Yangın için su püskürtücü cihazlar giriş katında ve diğer tüm katlarda bulunur. Su püskürtme cihazları, civardaki ısının içerisindeki asit tüpünün patlamasına neden olduğu durumda otomatik olarak çalışmaya başlar.
- Su püskürtme cihazlarına suyu sağlayacak su tankları ve su vanaları bulundurulur. Gerektiğinde kullanılmak üzere tahliye sistemleri konulur.
- Alarm aktive edildiğinde, tüm asansörler zemin kata döner ve kapıları açık bir halde işlev dışı kalır. Her kat bölümlere ayrılır ve yangın alarm sistemi yangının çıktığı katı, bölümü belirler. Bu bilgi güvenlik tarafından alarmın tetiklendiği yere bir an önce ulaşmak için kullanılır.
- Gerekli durumlarda insanların binaya girmesini ve binadan çıkmasını sağlayan zemin kattaki tüm geçiş kontrolleri pasif hale getirilir.
- Alarmın nedeninin incelenmesinin ardından yangın söndürme ekibi bina çalışanlarına, alarmın sebebi ve bu konuyla ilgili yapılması gerekenler ile ilgili bilgi verir.

5.19.5 Deprem Güvenliği

Yılda bir kez deprem tahliye tatbikatı yapılır

5.19.6 Yıldırım Güvenliği

Bina tepesine paratonerler yerleştirilir.

5.19.7 Hırsızlığa Karşı Güvenlik

- Varlıklar etiketlenir ve giren çıkan malzeme takip edilir.
- Her çeşit bilgi ve veri uygun şekilde sınıflandırılır ve kritikliğine göre ayrı kasa veya yerlerde saklanır.
- Bina girişlerine hırsız alarmı yerleştirilir.

5.19.8 Su Hasarı Güvenliği

Selden korunma: Bina uygun sel ve su tahliye kanallarına sahiptir. Binanın su sızıntısına karşı bakımı yaptırılır ve sızıntının tespit edilmesi durumunda önleyici önlemler alınır.

Sistem odasının yeri: Operasyon bölgesi ve sistem odası zemin katında daha yüksektedir. Sistem odasının fiziksel olarak bu lokasyon ihtiyaçlarını karşılayamadığı durumlarda, sistem odası ve içinde bulunan ekipmanlar için deprem ve su baskını tehditlerine karşı sigortalama yöntemi ile bu riskler transfer edilir. Bu şekilde su sızıntısından kaynaklanacak hasar riski düşürülür. Sistem odası duvarları pencerelerden uzaktır ve herhangi bir dış etkenden koruyacak şekilde izole edilir. Sistem odasındaki Bilgi İşlem donanımı su geçirmez dolaplar içerisinde muhafaza edilir.

Su tahliye sistemi: Su tahliye sistemi, suyun ve su tahliye boruları sistem odasından uzak olacak şekilde konumlandırılır.

5.19.9 Diğer

Zemin: Zemin yüksekliği bir adım yüksekliğindedir ve anti-statik malzemeyle döşelidir.

Prizler: Prizler topraklanır ve hatalı kablolama veya kısa devreye karşı güç kesicilerle desteklenir.

Konferans odası ve ziyaretçi odalarındaki hatların kısıtlanması: Konferans odası ve ziyaretçi odalarındaki tüm ağ hatları erişime kapalıdır. Gerekli görüldüğünde onay dâhilinde bu erişimler açılabilir.

Temizlik: Sistem odasına hiçbir şekilde yiyecek sokulmaz. Sunucu çevreleri temiz tutulur, çöp ve toz torbaları sunucuların yakınında tutulmaz.

Acil durum lambaları: Operasyon bölgesi ve diğer tüm bölgelerde, ani güç kesintilerinde gerekli olabilecek kendi kendine devreye giren acil durum lambaları vardır. Acil durum fenerleri, ışıkları ve havalandırmaları bulunmalıdır.

Acil durum güç kesimi: Stratejik bölümlerde, uygun etiketleme ve korumayla (yanlışlıkla çalıştırılmasına engel olmak amacıyla) acil durum güç kesim anahtarı bulunur.

6. İLGİLİ DOKÜMAN

- Bilgi Güvenliği Politikası
- İletişim ve Operasyon Yönetimi Politikası
- Ağ Güvenliği Politikası