**1. AMAÇ :**

Bu talimatın amacı, kurum personelinin ve kritik kurumsal bilgilerin korunması amacıyla sistem odasına, kurumsal bilgilerin bulundurulduğu sistemlerin yer aldığı tüm çalışma alanlarına ve kurum binalarına yetkisiz girişlerin yapılmasını önlemektir.

**2. KAPSAM :**

Bu talimat kurum binalarında yer alan bilgi varlıklarına erişim sağlayan tüm fiziksel güvenlik konularını, tüm veritabanı sistemlerini, kurumun sahip olduğu bütün sunucularını kapsamaktadır.

**3.SORUMLULAR :**

Bu talimatın uygulanmasından Başhekim, Tedavi ve Bakım Hizmetleri Müdürü, İdari ve Mali İşler Müdürü, Bilgi İşlem Sorumlusu sorumludur.

**4.FAALİYET AKIŞI**

**4.1. Fiziksel Güvenlik**

- Kurumun binalarının fiziksel olarak korunması, farklı koruma mekanizmaları ile donatılması temin edilmelidir.
- Kurumsal bilgi varlıklarının dağılımı ve bulundurulan bilgilerin kritiklik seviyelerine göre binalarda ve çalışma alanlarında farklı güvenlik bölgeleri tanımlanmalı ve erişim izinleri bu doğrultuda belirlenerek gerekli kontrol altyapıları teşkil edilmelidir.
- Kurum dışı ziyaretçilerin ve yetkisiz personelin güvenli alanlara girişi yetkili güvenlik görevlileri gözetiminde gerçekleştirilmelidir.
- Kritik bilgilerin bulunduğu alanlara girişlerin kontrolü akıllı kartlar veya farklı sistemler ile yapılmalı ve izlenmelidir.
- Tanımlanan farklı güvenlik bölgelerine erişim yetkilerinin güncelliği sağlanmalıdır. Personel kimliği ve yetkilerini belirten kartların ve ziyaretçi kartlarının düzenli olarak taşınması sağlanmalıdır.
- Kritik sistemler özel sistem odalarında tutulmalıdır.
- Sistem odaları elektrik kesintilerine ve voltaj değişikliklerine karşı korunmalı, yangın ve benzer felaketlere karşı koruma altına alınmalıdır.
- Fotokopi, yazıcı vs türü cihazlar mesai saatleri dışında kullanıma kapatılmalı, mesai saatleri içerisinde yetkisiz kullanıma karşı koruma altına alınmalıdır.

- Kuruma giriş yapacak ziyaretçi veya kurye teslimatların gerekli fiziksel güvenlik kontrollerinden geçirildikten sonra geçişine izin verilmelidir.
- Çalışma alanlarının kullanılmadıkları zamanlarda kilitli ve kontrol altında tutulması temin edilmelidir.
- Fotoğraf, video, ses vb kayıt cihazlarının yetki verilmeyen kişiler tarafından güvenli alanlara sokulmasının yasaklanmalıdır.

**4.2.Veri Tabanı Güvenliği:**

Veritabanı sistemleri envanteri ve bu envanterden sorumlu personel tanımlanmalı ve dokümante edilmelidir.

- Veritabanı işletim kuralları belirlenmeli ve dokümante edilmelidir.
- Veritabanı sistem logları tutulmalı ve izlenmelidir.
- Veritabanı sistemlerinde tutulan bilgiler sınıflandırılmalı ve uygun yedekleme politikaları oluşturulmalı, yedeklemeden sorumlu sistem yöneticileri belirlenmeli ve yedeklerin düzenli alınması kontrol altında tutulmalıdır.
- Yedekleme planları dokümante edilmelidir.
- Veritabanı erişim politikaları "kimlik doğrulama ve yetkilendirme" politikaları çerçevesinde oluşturulmalıdır.
- Hatadan arındırma, bilgileri yedekten dönme kuralları "acil durum yönetimi" politikalarına uygun olarak oluşturulmalı ve dokümante edilmelidir.
- Bilgilerin saklandığı sistemler fiziksel güvenliği sağlanmış sistem odalarında tutulmalıdır.
- Veritabanı sistemlerinde oluşacak problemlere yönelik bakım, onarım çalışmaları yetkili bir personel gözetiminde yapılmalıdır.
- Yama ve güncelleme çalışmaları yapılmadan önce bildirimde bulunulmalı ve sonrasında ilgili uygulama kontrolleri gerçekleştirilmelidir.
- Bilgi saklama ortamlarının kurum dışına çıkarılması için yetkilendirme yapılması ve bu durumun izleme takip amacıyla kaydedilmesi gerekir.
- Sistem dokümantasyonu güvenli şekilde saklanmalıdır.
- İşletme sırasında ortaya çıkan beklenmedik durum ve teknik problemlerde destek için kurulacak temaslar belirlenmelidir.

**4.3.Sunucu güvenliği**

**4.3.1. Sahip Olma ve Sorumluluklar**

Kurum bünyesindeki bütün dahili sunucuların yönetiminden sistem yöneticileri sorumludur. Sunucu konfigurasyonları sadece bu grup tarafından yapılacaktır. Bütün bilgiler tek bir merkezde güncel olarak tutulmalıdır.

Bütün sunucular ilgili kurumun yönetim sistemine kayıt olmalıdır. En az aşağıdaki bilgileri içermelidir.

*Sunucuların yeri ve sorumlu kişi.

*Donanım ve işletim sistemi.

*Ana görevi ve üzerinde çalışan uygulamalar.

*İşletim sistemi versiyonları ve yamalar.

**4.3.2. Genel Konfigurasyon Kuralları**

İşletim sistemi konfigurasyonları Bilgi İşlem Sorumlusunun talimatlarına göre yapılacaktır. Kullanılmayan servisler ve uygulamalar kapatılacaktır. Eğer mümkünse servislere erişimler için log tutulacaktır.Sunucu üzerinde çalışan işletim sistemlerinin, hizmet sunucu yazılımlarının ve anti-virüs vb. koruma amaçlı yazılımların sürekli güncellenmesi sağlanmalıdır. Mümkünse, yama ve anti virüs güncellemeleri otomatik olarak yazılımlar tarafından yapılmalı, ancak değişiklik yönetimi kuralları çerçevesinde bir onay ve test mekanizmasından geçirildikten sonra uygulanmalıdır. Uygulama erişimleri için standart güvenlik prensiplerini çalıştırın, gereksiz servisleri açmayın.

Sistem yöneticileri gerekli olmadığı durumlar dışında “Administrator” ve “root” gibi genel kullanıcı hesapları kullanmamalı, gerekli yetkilerin verildiği kendi kullanıcı hesaplarını kullanmalıdır. Genel yönetici hesapları yeniden adlandırılmalıdır. Gerekli olduğunda önce kendi hesapları ile log-on olup, daha sonra genel yönetici hesaplarına geçiş yapmalıdırlar. Ayrıcalıklı bağlantılar teknik olarak mümkünse güvenli kanal (SSH veya IPSec VPN gibi şifrelenmiş ağ) üzerinden yapılmalıdır.

Sunucular fiziksel olarak erişim kontrollü sistem odalarında bulunmalıdırlar. Sistem odasına bilgi yönetim sorumlusu ve bilgi yönetim çalışanı dışında başka kişilerin girişi yasaklanmıştır.

**4.3.3. Gözlemleme**

Kritik sistemlerde oluşan bütün güvenlikle ilgili olaylar loglanmalıdır ve aşağıdaki şekilde saklanmalıdır.

* Bütün güvenlikle ilgili loglar minimum 1 hafta saklanmalıdır ve online olarak erişilmelidir.

* Aylık full backuplar en az 6 ay tutulmalıdır.

Güvenlikle ilgili loglar sorumlu kişi tarafından değerlendirilecek ve gerekli tedbirleri alacaktır. Güvenlikle ilgili olaylar aşağıdaki gibi olabilir fakat bunlarla sınırlı değildir.

* Port tarama atakları.

* Yetkisiz kişilerin ayrıcalıklı hesaplara erişmeye çalışması.

*Sunucuda meydana gelen mevcut uygulama ile alakalı olmayan anormal olaylar.

**4.3.4. Uygunluk**

Denetimler yetkili organizasyonlar tarafından Kurum bünyesinde belli aralıklarda yapılacaktır. Denetimler Bilgi İşlem grubu tarafından yönetilecektir. Denetimler organizasyonun işleyişine zarar vermemesi için

maksimum gayret gösterilecektir.

**4.3.5. İşletim**

Sunucular elektrik ve ağ altyapısı ile sıcaklık ve nem değerleri düzenlenmiş ortamlarda işletilmelidir. Sunucuların yazılım ve donanım bakımları üretici tarafından belirlenmiş aralıklarla, yetkili uzmanlar tarafından yapılmalıdır. Sistem odalarına yetkisiz girişler engellenmelidir. Sistem odalarına giriş ve çıkışlar erişim kontrollü olmalı ve kayıt edilmelidir.

| Hazırlayan | Kontrol Eden | Onaylayan |
|---|---|---|
| Kalite & Akreditasyon Sorumlusu Kardelen ASMA | Kalite Koordinatörü Yeşim İNCİ | Kalite Yönetim Direktörü Prof. Dr. Tuncay ÇAĞLAR |