## 1. AMAÇ

Bu prosedür, Karamanoğlu Mehmetbey Üniversitesi Bilgi İşlem Daire Başkanlığı uyum kurallarını oluşturmayı amaçlar.

## 2. KAPSAM

Bu prosedür, Karamanoğlu Mehmetbey Üniversitesinin Bilgi İşlem Daire Başkanlığı uyum işlerinin tamamını kapsar.

## 3. SORUMLULAR

- Bilgi İşlem Daire Başkanlığı

## 4. TANIMLAR

## 5. UYGULAMA

### 5.1 Yasal Gereksinimlere Uyum

#### 5.1.1 İlgili Kanunların Belirlenmesi

Kurum'a ait olan yasalar, yönetmelikler ve sözleşmeler sonucunda ortaya çıkan yükümlülükler için hukuk bölümünün görüş ve onayı alınır. İş birimi yöneticisi, kendi temsil ettiği iş birimi için bu yükümlülüklerin, bunlara sebep olan yasaların, yönetmeliklerin ve sözleşmelerin, bunları yerine getirmek için uygulanan kontrolleri tespit ederek Bilgi Güvenliği Yöneticisi'ne iletilir. Bu kayıtların genel koordinasyonu Bilgi Güvenliği Yöneticisi tarafından gerçekleştirilir. Hukuk bölümü, İK departmanının ve Bilgi Güvenliği Yöneticisi'nin desteği ile çalışanları yasal gereksinimler ve bu gereksinimlere uyum üzerine bilgilendirir. Hukuk bölümü, ayrıca, yasa ve yönetmeliklere uyulmasını sağlamak için kontrollerin hızla uygulanmaya başlandığını takip eder. Uyumla ilgili hususlarda gerçekleştirilen denetimlerle birlikte uyum konuları konusunda da Hukuk bölümünden bilgi alınır.

### 5.2 Kuruluş Kayıtlarının Korunması

Bkz. Fiziksel Güvenlik ve Varlık Yönetimi Politika ve Prosedürleri

#### 5.2.1 Bilgi İşlem tesislerinin yanlış kullanımının önüne geçilmesi

Bkz. İnsan Kaynakları Güvenliği

## 5.3 Güvenlik Politikası ve Teknik Uyumun Bağımsız Kişiler Tarafından Gözden Geçirilmesi

### 5.3.1 Güvenlik politikalarına ve standartlarına uyum

Aşağıdakipolitikaveprosedürlereuyumdüzenliolarakgözdengeçirilir:

- Varlık Yönetimi
- İnsan Kaynakları Güvenliği
- Fiziksel ve Çevresel güvenlik
- İletişim ve Operasyon Yönetimi
- Sistem Planlama ve Kabulü
- Yedekleme ve Kurtarma
- Tedarikçi Yönetimi
- Erişim Kontrolü
- Ağ Güvenliği
- Bilişim Sistemi Alımı, Geliştirme ve Bakımı
- Şifreleme Sistemleri
- Olay Yönetimi
- İş Sürekliliği Yönetimi
- Uyum

### 5.3.2 Teknik Uyumun Kontrolü

Kullanılan sistemler, tanımlanan standartlarla uyumun kontrol edilmesi için Bilgi İşlem personeli tarafından düzenli olarak izlenir. Her çeyrekte bir defa kullanıcıların yalnızca kendilerine verilen yetkiler ile işlem yaptığı kontrol edilir. Senede bir defa da o yetkinliğe sahip bir üçüncü parti tarafından teknik anlamda gözden geçirme yapılır.

Uyum için kontrol edilecek noktalar şunlardır:

- Erişim kısıtlamaları
- Normal dışı bir kullanımın veya yeniden kullanıma açılan kullanıcı hesaplarının saptanması için sisteme giriş yollarının gözden geçirilmesi
- Yüksek yetkili kullanıcı hesaplarının kullanımı ve oluşturulması
- Seçilen işlemlerin izlenmesi
- Hassas kaynakların kullanımı

Uyum kontrolünün bulguları Bilgi Güvenliği Yöneticisi'ne raporlanır.

## 5.4 Bilgi Güvenliği Denetimi

### 5.4.1 Denetim Planının Hazırlanması ve Denetimlerin Gerçekleştirilmesi

İç denetim hizmeti iç veya dış kaynaktan alınacak şekilde planlanır. Bilgi Güvenliği Yöneticisi Denetimi gerçekleştirecek ekip, Bilgi Güvenliği Yöneticisi'nden aldıkları bilgi ve dokümanlar doğrultusunda Bilgi Güvenliği Politika ve Prosedürleri'nin (BGPP) senelik denetim planını hazırlar. Gerçekleştirilecek denetim BGPP kontrollerinin denetimini ve bilişim sistemleri ve herhangi bir yeni teknoloji veya yeni açılan hizmet kanalı gibi teknoloji ve hizmetlerin teknik testlerini içerir. Denetim planında bir değişiklik olduğunda, denetim ekibi güncellenmiş denetim planını hazırlar. Bilişim sistemlerinin teknik testi için öncesinde Varlık Sahibi ve Bilgi Güvenliği Yöneticisi'nden onay alınır. Teknik teste geçilmeden önce uygun önlemler alınır. Test araçları Bilgi Güvenliği Yöneticisi'nin gözetimindedir ve Bilgi Güvenliği Yöneticisi bu araçları hem fiziksel hem de mantıksal olarak korur. Denetimler yetkin ve bağımsız üçüncü partiler tarafından ya da Kurum içerisindeki bir iç denetim birimince gerçekleştirilebilir. Bilgi Güvenliği Yöneticisi ve Bilgi Güvenliği Yöneticisi denetçilere, denetim kapsamındaki alanlarda, gerekli bilgiyi ve Denetim Raporlama Formatları'nı sağlar.

### 5.4.2 Denetim Raporları, Bulgular ve Uygunsuzluklar

Denetçiler denetimi gerçekleştirir ve uygunsuzlukları ve gözlemlerini/önerilerini raporlarında sunarlar. Bilgi Güvenliği Yöneticisi denetim raporlarını temin eder ve gözden geçirir. Bilgi Güvenliği Yöneticisi aynı zamanda uygunsuzluk özet raporunu hazırlar. Bilgi Güvenliği Yöneticisi tarafından hazırlanan uygunsuzluk raporu Bilgi Güvenliği Yöneticisi Güvenlik Kurulu'na sunulur. Bilgi İşlem, IK veya İdari İşler gibi ilgili bölümler uygunsuzlukların kapatılması için düzeltici ve önleyici faaliyetler başlatır ve bunların belirlenen sürelerde sonuçlanmasını sağlar. Belirlenen süre sonunda, Bilgi Güvenliği Yöneticisi uygunsuzlukların giderildiğini onaylar veya uygunsuzlukları kendi kapatır. Değerlendirmeyi yapan kişi uygunsuzluk özet raporunu güncelleyecek olan denetim ekibine bulguları raporlar.

### 5.4.3 Denetim Planlarındaki Değişiklikler

Kuruluştaki değişikliklere göre Bilgi Güvenliği Yöneticisi denetim planında gerekli değişiklikleri yapar. Bilgi Güvenliği Yöneticisi ayrıca Düzeltici ve/veya Önleyici faaliyetlerin başlamasını sağlar.

## 5.5 Teknik Zafiyet Değerlendirmesi

- Birçok zayıflık değerlendirmesinde kullanılmak üzere, Kurum kritik varlıklarını detaylandıran bir varlık listesi oluşturulacaktır.

- Senede iki kere Kurum kritik varlıklarına yönelik, Kurum içi teknik zafiyet değerlendirmesi gerçekleştirilir.
- Eğer uygun uzmanlık ve ekip tesis edilebilirse kuruluş içinden bir ekip tarafından senede bir kere bu varlıkların sızma testleri yapılır.
- Bir dış Kurum ya da kuruluşa, Kurum'un kritik varlık listesi için her yıl bağımsız zafiyet ve sızma testleri yaptırılır.
- Zafiyetler tanımlandığında, bunlar Güvenlik Kurulu'na sunulur ve iş etkisine göre önceliklendirilir.
- Bilgi Güvenliği Yöneticisi, en yüksek öncelikliden başlayarak açıklıkların kapatılmasını teftiş eder. Tanımlanan her bir zafiyetin giderilmesi için bir zaman çizelgesi oluşturulur.
- İyileştirmenin mümkün olmadığı durumlarda riskler en aza indirgenir ve arta kalan risk dokümante edilir.

## 6. İLGİLİ DOKÜMAN

- Uyum Politikası