Lokman Hekim Üniversitesi

Bilgi Güvenliği Yönetim Sistemi

Bilgi Güvenliği Alt Politikaları

KURUMA ÖZEL

İÇİNDEKİLER

1. Amaç

Bu doküman, Kapsam Analizi Dokümanında belirtilen birimlerde tüm bilgi varlıklarının güvenliğinin sağlanması, BGYS'nin kurulması, işletilmesi, sürdürülmesi ve sürekli iyileştirilmesi için yönetimin yönlendirmesi ve desteğinin belirlenmesi amacı ile oluşturulmuştur.

2. Kapsam

Bu doküman, kapsamdaki tüm bilgi varlıklarını ve bilgi varlıklarının güvenliğini kapsamaktadır.

3. Revizyon Kayıtları

Revizyon No	Tarih	Revizyon Nedeni	Revizyon Sayfa No	Revize Edilen Bölüm

4. Tanımlamalar ve Kısaltmalar

Bu dokümandaki kısaltma ve tanımlar, Kısaltmalar ve Tanımlar Kılavuzunda açıklanmaktadır.

5. Uygulama

5.1. Erişim Kontrol Politikası

Bilgi güvenliğini sağlamanın en temel yolu, bilgi varlığına yetkisiz kişilerin erişimlerini engellemek ve yetkisi olan kişilerin erişimlerini de ihtiyaca göre kısıtlamaktır. Bu erişimler, fiziksel ve mantıksal erişim olarak iki şekilde denetlenir. Erişim kontrollerinde yasal gereksinimler göz önünde bulundurulur ve varlık sınıflandırmasına uygun yetkilendirmeler

yapılır. Gerektiği kadar bilme prensibi ve açıkça izin verilmedikçe her şey yasaktır kuralı Kurum erişim yönetiminin temelini oluşturur.

5.2. Varlıkların Kabul Edilebilir Kullanımı

Kurum iş süreçlerinin yürütülmesinde yalnızca kurum bilişim kaynakları kullanılır. Bu kaynakların kullanımında esas, Lokman Hekim Üniversitesi'nin eğitim, öğretim, araştırma, geliştirme, toplumsal hizmet ve idari/yönetimsel faaliyetleri ile doğrudan ilişkili olan kullanımdır. Kurum kaynaklarının kullanımı, mevzuata ve Kurum politika ve prosedürlerine aykırı olamaz. Varlıkların kullanımında yasal gereksinimler, gizlilik, bütünlük ve erişilebilirlik kavramları göz önünde bulundurularak güvenlik riskleri incelenir ve önlemler alınır.

5.3. İnsan Kaynakları Disiplin Kuralları

Tüm personele mevzuat gereği ve Kurum Bilgi Güvenliği politika, prosedür, talimat, taahhütname vb. şartlarına uymadığında İnsan Kaynakları Güvenliği Prosedürüne uygun disiplin süreci başlatılır.

5.4. Parola Politikası

Kurumda kullanılan tüm parolalar uluslararası standartlara uygun güvenlik seviyeleri göz önünde bulundurularak belirlenir ve kullanılır. Belirlenen bu seviye tüm parola gerektiren sistemlerde uygulanır. Parolanın kişiye özel olduğu paylaşılmaması ve tahmin edilemez olması kullanıcıların sorumluluğundadır.

5.5. Temiz Masa Temiz Ekran Politikası

Gizli ve üzeri bilgi sınıfındaki evraklar, parolalar, taşınabilir depolama ortamları, bilgi ve belgeler masa üzerinde, yazıcı veya faks gibi cihazlarda ya da kolayca ulaşılabilir yerlerde bırakılmaz. Tüm çalışanlar kendi masalarının temizliği ve düzeninden sorumludur. Kullanımı biten basılı evraklar kırpma makinesi ile kırpılarak imha edilir. Terk edilmiş masaların üzerinde not kağıtları, kişisel ajandalar ve işle ilgili dokümanlar bırakılmamlıdır. Bilgisayar ekranlarında kuruma ait çalışma dosyaları, klasörler, herhangi bir formatta bilgi içeren dosyalar ve bunlara ait kısa yollar bulundurulmamalıdır. Personelin kullandığı masaüstü veya dizüstü bilgisayarların iş sonunda ya da masa terkedilecekse ekran kilitlenerek çalışma ortamlarında veri güvenliği şartlarını kontrol etmek personel sorumluluğundadır. Şifre, parola gibi kimseye söylenmemesi gereken gizli bilgiler hiçbir suretle masa üzerindeki bir dosyaya yazılmamalı, ekranın üzerine not şeklinde yapıştırılmamalıdır.

5.6. Güvenli Geliştirme Politikası

Kurumda kullanılacak uygulamaların ve sistemlerin seçiminde ve geliştirmesinde dünya çapında kabul görmüş standartların uygulanması ya da bu standartlara uygun olan uygulama ve sistemlerin temini sağlanır. Bu bağlamda; Geliştirme yaşam döngüsü içerisindeki sistem değişikliklerinin kontrolü, işletim platformu değişikliklerinin kontrolü, yazılım paketlerindeki değişikliklerin kontrolü, güvenli sitem mühendisliği prensipleri, Güvenli geliştirme ortamı, sistem güvenlik testleri, sistem kabul testleri, test verisinin güvenliği kontrolleri uygulanır.

5.7. Mobil Cihaz Kullanımı Politikası

Mobil cihazların kullanımından kaynaklanan risklerin yönetimi için fiziksel ve mantıksal erişime uygun güvenlik önlemleri alınır. Mobil cihazlar mümkün olduğunca halka açık alanlarda kullanılmaz. Yetkisiz erişim ve bilgi ifşasını engelleyecek kontroller uygulanır. Bu kontroller kriptografik önlemler, kimlik doğrulama mekanizmaları ve fiziksel muhafazadır.

5.8. Bilgi Transfer Politikaları

Bilgi transferinde varlık sınıflarına uygun olarak güvenli paylaşım yöntemleri kullanılır. Şifahi olarak gizlilik dereceli bilgilerin kurum içinde ve dışında aktarımı söz konusu olamaz. Kurumsal verilerin paylaşımı sadece Kurum kaynakları kullanılarak yapılır. Kurum içi ve dışı veri paylaşımı için mevzuat ya da sözleşme ile paylaşım gereksinimlerinin belirlenmiş olması gerekir.

5.9. Tedarikçi İlişkileri Bilgi Güvenliği Politikası

Kurum, iş süreçlerinin işleyişini, devamlılığını ve kalitesini arttırmak için tedarikçiler ile çalışmalar yapmaktadır. Yapılan bu çalışmalar esnasında çalışma şartlarının belirlenmesi ve dokümante edilmesi hem Kurumun hem de tedarikçinin sorumluluğundadır.

Tedarikçi ilişkilerini yönetmek için, alınan mal ya da hizmetler bilgi güvenliğini etkileyecek türde ise, her birim kendi risk eğilimine ve çalışacağı tedarikçinin türüne göre tedarik sürecini planlar. Süreç dâhilinde bilgi varlıklarına erişim türünü belirler, verilen erişim izinlerini izler, Kurum politika ve prosedürlerine uyumu sağlar ve bilgi güvenliği farkındalığını arttırmak için gerekli uygulamaları gerçekleştirir.

Tedarikçi anlaşmaları ile Kurum ve tedarikçi arasında yanlış anlama olasılığının ortadan kaldırılmasını sağlamak ve bilgi güvenliği gereksinimlerini yerine getirmek için her iki tarafın da yükümlülüklerine ilişkin dokümante edilmiş belge oluşturulur ve saklanır.

6. İlgili Dokümanlar

6.1. İç Kaynaklı Dokümanlar

1. Kapsam Analizi Dokümanı
2. Kısaltmalar ve Tanımlar Kılavuzu

6.2. Dış Kaynaklı Dokümanlar

1. TS EN ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı