MAKÜ

BURDUR MEHMET AKİF ERSOY ÜNİVERSİTESİ

# BİLGİ GÜVENLİĞİ İHLAL OLAYI YÖNETİMİ PROSEDÜRÜ

# İçindekiler

# 1 Amaç

Bu dokümanın amacı bilgi güvenliği ihlal olayları tespitinde ve yönetiminde dikkat edilmesi gereken noktaları açıklamaktır.

# 2 Kapsam

Bu doküman Bilgi Güvenliği Kapsamı dokümanında yer alan tüm bilgi varlıklarını içerir.

# 3 Sorumluluk

| Görev / Rol/Unvan | Dokümanın Hazırlanması | Dokümanın Kontrolü | Dokümanın Onaylanması | Dokümanın Yayınlanması | Dokümanın Güncellenmesi | Dokümanın Uygulanması | Dokümanın Uygulamadan Kaldırılması |
|---|---|---|---|---|---|---|---|
| **Üst Yönetim** | | | X | | | X | X |
| **Üst Yönetim Temsilcisi** | | | X | | | X | X |
| **BGYS Yöneticisi** | X | X | | X | X | X | |
| **BGYS Birim Sorumlusu** | X | X | | | | X | |
| **Diğer Çalışanlar** | | | | | | X | |

# 4 Tanımlamalar ve Kısaltmalar

| Terim | Tanım/Açıklama |
|---|---|
| **Kurum** | Kuruluşumuzun Kapsam Analizi Dokümanı'nda belirtilen birimleri |
| **BGYS** | Bilgi Güvenliği Yönetim Sistemi |
| **BGYS Yazılımı** | Bilgi Güvenliği Yönetim Sisteminin genel yönetiminin yapıldığı uygulamadır. |

# 5 İşlem Detayı

## 5.1 Sorumluluklar

Bilgi güvenliği ihlal olayı tespiti konusunda tüm çalışanlar öncelikli ve gerçek sorumludurlar. Bununla birlikte tüm kullanıcılar sistemde oluşan olağan dışı durumları Yardım Masası üzerinden bildirmekle sorumludurlar.

BGYS Yöneticisi olayların tespitinden sonraki süreçler olan delil toplama, önlem alma, deneyim edinme ve disiplin yönetimi konularında çalışma gerçekleştirecektir. İhlal olayları ile ilgili oluşturulan kayıtlar bilgi güvenliği toplantılarında BGYS sorumluları ile paylaşılacaktır.

BGYS Sorumluları tekrar edebilecek ihlal olaylarını engellemek veya gerçekleşmesi durumunda müdahale edebilmek için İhlal olayları ile ilgili oluşturulan kayıtları incelemek ile sorumludur.

BGYS Yöneticisi olayların tespitinde kendi elde ettiği bilgileri veya başkaları tarafından onay verilen bilgileri alıp, bunların bir bilgi güvenliği ihlal olayı olup olmadığını karar vermekle sorumludur.

Tespiti yapılan olay ile ilgili kurum dışı birim ya da firma / kurumdan destek alınması gereken durumlarda iletişimi kurmak ve sağlamak konusunda öncelikli sorumluluk müdahaleyi yapacak olan ilgili birim BGYS Sorumlusudur.

## 5.2 Bilgi Güvenliği İhlal Olayları Yönetimi

### 5.2.1 Tespit

Kurum çalışanlarının şüpheli buldukları durumlarda acil bir şekilde olay bildirimi yaparak iletişime geçmeleri gereklidir. İstem dışı kaybolan veya ortaya çıkan dosyalar, anti-virüs ajanının çalışmasında çıkan sorunlar, bilgisayarların aşırı yavaşlaması, istemsiz çalışan programlar ve istemsiz açılan pencereler, yetkisiz personelin güvenli alanlarda bulunması, gizli dosyaların dış müdahaleye açık olması gibi çok özel durumlarda da acil bir şekilde olay bildirimi yaparak bilgilendirme yapılır.

BGYS Yöneticisi düzenli bir şekilde aşağıdaki kontrollerin uygulanmasını sağlayarak bir bilgi güvenliği ihlal olayı oluşmasını kontrol etmelidir.

- Fiziksel olarak sistem ve servislerde açıklıkların bulunup bulunmadığı kontrol edilmelidir.
- Sistem güvenlik yazılımları
- Erişim denetim politikasına göre erişim denetimi sırasında tespit edilen farklı yetkiler ve kullanıcılar.
- Dokümantasyona uygun uygulanmayan işlemler.

BGYS yöneticisi ve BGYS Sorumluları tarafından ihlal olaylarının tespiti için "**Bilgi Güvenliği Olay Bildirim Formu**" doldurulur.

### 5.2.2 Değerlendirme

Bilgi güvenliği ihlal olayı tespiti sonrası olayla ilgili deliller toplanmalıdır. Müdahaleden önce kayıtların toplanması, bozulması engellenecek şekilde saklanması ve yetkisiz erişime karşı korunmasından BGYS Yöneticisi sorumludur.

### 5.2.3 Müdahale

Kontroller veya bildirilen durumlar ile tespit edilen ve delilleri toplanan tüm olaylar için diğer işlemlerden önce olaya sebep olan zafiyet düzeltilmedir.

Zafiyetlerin kapatılmasından sonra mutlaka kontroller tekrarlanmalı ve zafiyetin kapandığı onaylanmalıdır. Delilleri tahrip edecek veya bozacak hiçbir açıklık için kapatma işlemi gerçekleştirilmemelidir.

Risk seviyesi çok yüksek olaylar için sistemler tamamen kapatılmalı veya diğer sistemlere erişimi engellenmelidir.

Bilgi güvenliği ihlal olayına yapılan müdahaleler Matbuu formlar üzerinden takip edilerek olay yönetimi, deneyim edinme ve önlem alma amacıyla kayıt altına alınmalıdır. Bilgi güvenliği ihlali kapsamında tespit edilen olayları yönetmek için kök neden analizi gerekiyor ise düzeltici faaliyet (DF) açılmalıdır, kök neden analizi gerekmiyor ise işlem yapılıp bilgi güvenliği ihlal olayı rapor formuna kayıt edilmelidir. Kök neden analizinin yapılıp yapılmamasına BGYS yöneticisi karar verir.

- Gelen ihlal olayları bildirimlerine en kısa sürede delil toplanarak müdahale edilir.
- Olaya müdahale konusunda yeterli yetkinlik bilgi ve beceriye sahip olunmaması durumunda kurum içi veya kurum dışı ilgili çalışan ya da 3. tarafla iletişime geçilir.
- Tespit edilen olay felaket kapsamında değerlendirilecek kapsamda ise (yangın, sel, sabotaj vb.) “Bilgi Güvenliği Sürekliliği Yönetimi Prosedürü” uygulanacaktır.
- İhlal olayı için işlemlerden önce kanıtlar toplanmalıdır.
- Risk oluşturan varlık en kısa süre içeresinde zarar verebileceği ortamdan uzaklaştırılmalı veya ayrılmalıdır.
- Kontroller sonucunda tespit edilen olaylar için mutlaka belirli bir süre daha benzer kontroller tekrarlanmalıdır.
- Müdahale esnasında raporlama için gerekli zafiyet analizi, adli analiz, maliyet tespiti ve ihlal sebepleri gibi veriler toplanacaktır.

### 5.2.4 Önlem alma ve Ders Çıkarma

Tespit edilen her bir olay için tekrar oluşmasını engellemek için önlemler alınmalıdır.

Ders çıkarma herhangi bir ihlal olayının tekrarlanmamasını veya tekrar oluştuğunda soruna daha kısa sürede çözüm bulunmasını amaçlar.

- Bir güvenlik ihlal olayına önlem almak için aşağıdaki işlemlerden herhangi biri uygulanabilir. Yapılan işlemler mutlaka kayıt altına alınmalıdır.
- Oluşturulan kayıtlar incelenmeli ve çözüm yolları ve çözümler için gerekli iletişim bilgileri kayıt edilmelidir.
- Yanlış uygulamalardan kaynaklı olaylar için mutlaka yazılı prosedürler oluşturulmalıdır.
- Prosedürlerden kaynaklanan olaylar için prosedürler tekrar gözden geçirilmeli ve düzeltilmelidir.
- Fiziksel açıklıklardan kaynaklı olaylar için fiziksel önlemler veya ek projeler gerçekleştirilmelidir.
- Kurum içerisinde çalışmalar ile çözülmeyecek olaylar için ek projeler yapılmalı ve alımlar gerçekleştirilmelidir.
- Erişim kaynaklı sorunlar için erişimler tekrar denetlenmeli, diğer benzeri erişim yetkileri de kontrol edilmelidir.
- Yazılım ve uygulamalardan kaynaklı olaylarda güncelleştirmeler kontrol edilmeli, açıklılar güncelleştirme, ek yama geliştirme gibi yöntemler ile kapatılmalıdır.
- Fiziksel teçhizatlardan kaynaklı sorunlar için alınan önlemler tüm diğer benzer teçhizatlarda da uygulanmalıdır.
- Virüs, Trojan veya zararlı kodlardan kaynaklı olaylar için sorun kaynağı tespit edilmeli, güvenlik yazılımlarını niye yeterli olmadığı irdelenmelidir. Bulunan önlemler mutlaka tüm sisteme uygulanmalıdır.

### 5.2.5 Kayıt ve Kanıt Toplama

Olayın tespiti ve sorumlunun belirleneceği aşağıdaki kayıtların bütünlüğünün bozulmadığı kontrol edilmelidir. Bilgi güvenliği ihlal olayları için toplanan deliller 3 yıl boyunca silinmemelidir

- Sorumlu tespiti ile ilgili durumlarda kamera varsa mutlaka kamera kayıtları

- Erişim kayıtları
- Kontrol kayıtları
- Sistem güvenlik yazılımları tarafından tutulan kayıtlar
- Sorunların çözülmesi için gerekli maliyet kayıtları
- Bilgi güvenliği olaylarının değerlendirilmesi için ihtiyaç gösterebilecek ve gelecekteki olayların sıklığı, hasar ve maliyet sınırlarını belirleyecek kayıtlar

### 5.2.6 Disiplin İşlemleri

Deliller toplandıktan sonra sadece BGYS Yöneticisi ve BGYS Üst Yönetim Temsilcisi ve Üst Yönetim tarafından görülmeli ve disiplin sürecine göre başka kişiler ile paylaşılmalıdır. Disiplin işlemleri "**İnsan Kaynakları Güvenliği Prosedürü**" ne göre uygulanır.

# Revizyon Kayıtları

| Rev. No | Tarih | Hazırlayan | Revizyon Nedeni /Sayfa No | Onaylayan | İmza |
|---|---|---|---|---|---|
| **1** | | | | | |
| **2** | | | | | |
| **3** | | | | | |
| **4** | | | | | |
| **5** | | | | | |