|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **BİLGİ GÜVENLİĞİ**  **İHLAL BİLDİRİM VE YÖNETİMİ** | | | C:\Users\olympos\Desktop\antalya_ism_logo 800x600.jpg |
| **Kodu** | **Yayınlama tarihi** | **Revizyon Tarihi** | **Revizyon No** | **Sayfa** |
| **BG.PR.04** | **20.10.2015** | **20.10.2015** |  | **1/2** |

# AMAÇ

Antalya İl Sağlık Müdürlüğü ve müdürlüğe bağlı kurumlarda çalışan personelin bilgi güvenliği ihlali olması halinde kullanacağı ihlal bildirim formu ve ihlal bildirim yönetiminin belirlenmesi.

# KAPSAM

Bu politika, T.C. Sağlık Bakanlığı Antalya İl Sağlık Müdürlüğü bünyesinde ve bağlı kurumlarda çalışan tüm personeli kapsar.

# POLİTİKA METNİ

* 1. Bilginin gizlilik, bütünlük ve kullanılabilirlik açısından zarar görmesi, bilginin son kullanıcıya ulaşana kadar bozulması, değişikliğe uğraması ve başkaları tarafından ele geçirilmesi, yetkisiz erişim gibi güvenlik ihlali durumlarında mutlaka kayıt altına alınmalıdır.
  2. Bilgi güvenlik olayı raporlarının bildirilmesini, işlem yapılmasını ve işlemin sonlandırılmasını sağlayan uygun bir geri besleme süreci oluşturulmalıdır.
  3. Bilgi güvenliği ihlâli oluşması durumunda kişilerin tüm gerekli faaliyetleri hatırlamasını sağlamak maksadıyla bilgi güvenliği olayı rapor formatı hazırlanmalıdır.

1. Güvenlik olayının oluşması durumunda olay anında raporlanmalıdır.
2. İhlali yapan kullanıcı tespit edilmeli ve ihlalin suç unsuru içerip içermediği belirlenmelidir.
3. Güvenlik ihlaline neden olan çalışanlar, üçüncü taraflarla ilgili resmi bir disiplin sürecine başvurulur.
4. Tüm çalışanlar, üçüncü taraf kullanıcıları ve sözleşme tarafları bilgi güvenliği olayını önlemek maksadıyla güvenlik zayıflıklarını doğrudan kendi yönetimlerine veya hizmet sağlayıcılarına mümkün olan en kısa sürede rapor edilir.
5. Bilgi sistemi arızaları ve hizmet kayıpları, zararlı kodlar, dos atakları, tamamlanmamış veya yanlış iş verisinden kaynaklanan hatalar, gizlilik ve bütünlük ihlâlleri, bilgi sistemlerinin yanlış kullanımı gibi farklı bilgi güvenliği olaylarını bertaraf edecek tedbirler alınır.
6. Normal olasılık planlarına ilave olarak olayın tanımı ve sebebinin analizi, önleme, tekrarı önlemek maksadıyla düzeltici tedbirlerin planlanması ve uygulanması, olaylardan etkilenen veya olaylardan kurtulanlarla iletişim, eylemin ilgili otoritelere raporlanması konuları göz önüne alınır.
7. İç problem analizi, adli incelemeler veya üretici firmadan zararın telafi edilmesi için aynı türdeki olayların izleme kayıtları (log) toplanır ve korunur.
8. Güvenlik ihlallerinden kurtulmak için gereken eylemler, sistem hatalarının düzeltilmesi hususları dikkate alınır.
9. Bilgi güvenliği olaylarının değerlendirilmesi sonucunda edinilen bilgi ile edinilen tecrübe ve yeni kontrollerin oluşturulması, aynı olayın tekrar etmesini önleyecek veya yüksek etkili olayların oluşmasını engelleyecektir.
10. Kanıt toplama; kuruluş içerisinde disiplin faaliyeti için delil toplanırken uygulanacak genel kurallar şunlardır;

- Kanıtın mahkemede kullanılıp kullanılamayacağı ile ilgili kabul edilebilirlik derecesi,

- Kanıtın niteliği ve tamlığını gösteren ağırlığı.

1. Bilgi güvenliği politika, prosedür ve talimatlarına uyulmaması halinde, kurum Personel Yönetmeliği gereğince aşağıdaki yaptırımlardan bir ya da birden fazla maddesini uygulayabilir:

Uyarma, Kınama, Para cezası, Sözleşme feshi.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **BİLGİ GÜVENLİĞİ**  **İHLAL BİLDİRİM VE YÖNETİMİ** | | | C:\Users\olympos\Desktop\antalya_ism_logo 800x600.jpg |
| **Kodu** | **Yayınlama tarihi** | **Revizyon Tarihi** | **Revizyon No** | **Sayfa** |
| **BG.PO.01** | **20.10.2015** | **20.10.2015** |  | **2/2** |

**BİLGİ GÜVENLİĞİ İHLAL BİLDİRİM FORMU**

|  |  |  |
| --- | --- | --- |
| **İhlal Bildirimi Yapacak Kişinin** | | **Olay Derecesi**    Düşük Orta  Yüksek Kritik |
| Adı \* |  |
| Soyadı \* |  |
| Telefon \* |  |
| e-posta \* |  |
| Departman \* |  |
| Tarih \* |  |
| **Olay Tanımı**  Yetkisiz Giriş  Yazılım Arızası  Virüs / Solucan / Trojan  Web Sitesinin Hack Edilmesi  Tehdit / E-Posta Bombardımanı  Copyright Usülsüzlüğü  Fraud / Spam  Müstehcen veya Çirkin Mesaj Gelmesi  Tehdit / E-Posta Bombardımanı  Güvenlik Açıklarından Faydalanma  Diğer | | |
| **Olay Açıklaması** | | |

*(\*) Zorunlu alanlar*

*İhlal bildirimi resmi web sitemizden de yapılabilir. (*[*www.antalyasm.gov.tr*](http://www.antalyasm.gov.tr) *🡪 Bilgi Güvenliği 🡪 Bilgi Güvenliği İhlal Bildirim Formu)*

*İhlal bildirimi form şeklinde düzenlenecekse, bildirimi yapan kişinin ıslak imzası alınmalıdır.*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **HAZIRLAYAN**  **(Bilgi Güvenliği Komisyonu)** | | | | | | | |
| *Komisyon Başkanı*  Bülent YURTERİ  Şube Müdürü | *Başkan Yardımcısı*  Ersin HOŞER  V.H.K.İ | *Üye*  Okşan Duru ÖZDAĞ  Doktor | | | *Üye*  Demet KILIÇ  Avukat | *Üye*  Osman ÜNAY  Bilgisayar Mühendisi | *Üye*  K. Erkan AKKUŞ  Bilgisayar Mühendisi |
|  |  |  | | |  |  |  |
| *Üye (Eğitimci)*  Ünal GÖKÇE  Sağlık Memuru | *Bilgi Güvenliği Yetkilisi*  Özgür AYDIN  Programcı | *Üye*  Fethi ÇELİK  Programcı | | | *Üye*  İsmail ÇİFTÇİ  Bilgisayar İşletmeni | *Üye*  Okkan KARADAŞ  Tıbbi Sektreter |  |
|  |  | |  |  |  |  | |

**O N A Y**

…/…/2015

Dr. Ünal HÜLÜR

İl Sağlık Müdürü